# Ανοικτό Πανεπιστήμιο Κύπρου

## Σχολή Θετικών και Εφαρμοσμένων Επιστημών


## Μεταπτυχιακή Διατριβή
## στα Πληροφοριακά Συστήματα

# Προστασία προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση και νέες τεχνολογίες


**Μάιδα Μερόπη**

**Επιβλέπων Καθηγητής**
**Κωνσταντίνος Λιμνιώτης**


**ΙΑΝΟΥΑΡΙΟΣ 2014**

# Ανοικτό Πανεπιστήμιο Κύπρου

## Σχολή Θετικών και Εφαρμοσμένων Επιστημών


# Προστασία Προσωπικών Δεδομένων Στην Ευρωπαϊκή Ένωση Και Νέες Τεχνολογίες


**Μάιδα Μερόπη**

**Επιβλέπων Καθηγητής**
**Κωνσταντίνος Λιμνιώτης**


Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου


**ΔΕΚΕΜΒΡΙΟΣ 2013**

# Περίληψη

Με τη ραγδαία πρόοδο της τεχνολογίας και των νέων εφαρμογών, η εφαρμογή πολλών εκ των επιταγών της νομοθεσίας περί προστασίας των προσωπικών δεδομένων καθίσταται ιδιαίτερα δυσχερής. Θέματα όπως η ανάγκη λήψη ρητής συγκατάθεσης των χρηστών για την επεξεργασία των προσωπικών τους δεδομένων σε καθημερινές εφαρμογές πολύ συχνά «παρακάμπτονται» από τα διάφορα συστήματα/εφαρμογές, ενώ επίσης πολύ συχνά οι χρήστες δεν είναι πλήρως ενήμεροι για την ακριβή επεξεργασία των προσωπικών τους δεδομένων που λαμβάνει χώρα. . Περαιτέρω, με την εξάπλωση των ιστολογίων (blogs), του υπολογιστικού νέφους , των κοινωνικών δικτύων κτλ. η αποτελεσματική προστασία των προσωπικών δεδομένων, με ταυτόχρονη αξιοποίηση των πλεονεκτημάτων που παρέχουν οι τεχνολογίες αυτές, αποκτά ακόμη μεγαλύτερη βαρύτητα.

Η Ευρωπαϊκή Επιτροπή είναι σε διαδικασία αναθεώρησης της υπάρχουσας νομοθεσίας περί προστασίας προσωπικών δεδομένων (Οδηγία 95/46/ΕΚ, που έχει ενσωματωθεί στο ελληνικό Δίκαιο με το ν. 2472/1997), έχοντας εκδώσει ένα σχέδιο Κανονισμού διαθέσιμο προς διαβούλευση. Η νέα αυτή πρόταση εμφανίζεται ως πιο «αυστηρή», αναγνωρίζοντας σαφώς ακόμη περισσότερα δικαιώματα στους πολίτες για την προστασία των δεδομένων τους. Ωστόσο, η υλοποίηση των βασικών αρχών που διέπουν τη νέα αυτή πρόταση έχει ακόμα πολλά ανοιχτά ερωτήματα, τα οποία αποτελούν αναμφισβήτητα πρόκληση από την πλευρά της τεχνολογίας (για παράδειγμα, πώς μπορεί να εφαρμοστεί αποτελεσματικά το «δικαίωμα στη λήθη» στο σημερινό Internet;).

Τα ζητήματα που καλείται να αντιμετωπίσει η παρούσα διατριβή αποτελούν ήδη αντικείμενο μελέτης των ευρωπαϊκών αρχών Προστασίας Προσωπικών Δεδομένων καθώς και σχετικών Κοινοτικών Οργάνων (όπως ο Ευρωπαίος Επόπτης Προστασίας Προσωπικών Δεδομένων – EDPS). Ο υπό διαβούλευση νέος Κανονισμός για την Προστασία Προσωπικών Δεδομένων αποτελεί τρέχον αντικείμενο μελέτης εξαιρετικού ενδιαφέροντος, αφού για την εξεύρεση λύσεων και προτάσεων απαιτείται ταυτοχρόνως πολύ καλή γνώση της σχετικής νομοθεσίας αλλά και της τεχνολογίας της πληροφορικής (ιδιαίτερα δε της τεχνολογίας Διαδικτύου και ασφάλειας επικοινωνιών). Στην παρούσα διατριβή γίνεται μία επισκόπηση τόσο του ισχύοντος νομικού πλαισίου όσο και της προτεινόμενης αναθεώρησής του, με έμφαση στις τεχνολογικές προκλήσεις που ανακύπτουν και πώς αυτές μπορούν να αντιμετωπιστούν.

# Summary

With the rapid advance of the technology and the new applications, the implementation of many of the rules of the legislation about the protection of personal data is becoming increasingly difficult. Issues like the required oral consent of the users for the use of the personal data in everyday applications, are very often subsided by the various systems/applications (for example, is required the oral consent of the user for the acceptance of a "cookie" on his computer at the visit on a webpage or for the face recognition service and the upload of the relevant title from Facebook). Moreover, with the spread of the blogs, of the cloud computing, the social services, e.t.c, the effective protection of the personal data with the simultaneous benefit of the advantages of these technologies is becoming even more of grave importance. The European Union is at a procedure of revision of the existing legislation about the protection of personal data (Guideline 95/46/E.U. which was adopted within the Greek legislation with law 2472/1997), and has published a draft of a Regulation, available for public consideration. This new proposal appears to be more strict, recognizing clearly even more rights to the citizens for the protection of their rights, however the implementation of the fundamental principles that rule this proposal have still many questions open (For example how can the *Right to Be Forgotten* to be implemented within the present internet?)

The issues that this dissertation is dealing with, have already become an object of study by the European Authority for the Protection of the Personal Data and the other relevant European Authorities, like the European Data Protection Supervisor (EDPS). The new regulation about the Protection of the Personal Data which is under public consideration, is an object of study of great interest, since for the creation of the solutions and proposals requires both very good knowledge of the relevant legislation but also of the technology of informatics, (Especially of the internet technology and the security of communication)

Summary of the goal, the methods followed, and the results of the M.Sc. dissertation, as these are documented in the text of the M.Sc. dissertation that follows. The extent of the summary is limited to one page only. The summary should be given in English, and it should be a faithful translation of the summary provided in Greek in the previous page.

# Ευχαριστίες

Ένα μεγάλο ευχαριστώ στον επιβλέποντα καθηγητή μου Κωνσταντίνο Λιμνιώτη για την καθοδήγηση και την εν γένει υποστήριξή του.

Επίσης θα ήθελα να ευχαριστήσω τον άντρα μου και την οικογένεια μου για την απεριόριστη αγάπη και κατανόηση τους και ειδικά την μικρή μου κόρη Ειρήνη για όλες τις ώρες που με στερήθηκε από κοντά της.

# Περιεχόμενα

# Κεφάλαιο 1
# Εισαγωγή

Η έννοια της προστασίας των προσωπικών δεδομένων, η οποία είναι στενά συνυφασμένη με την ιδιωτικότητα, αποτελεί αναμφίβολα ένα ιδιαίτερα σημαντικό ζήτημα το οποίο, με την εξέλιξη της τεχνολογίας, αποκτά ακόμη πιο ιδιαίτερα χαρακτηριστικά. Εξάλλου, η βαθύτερη έννοια της ιδιωτικότητας, η οποία αποτελεί ένα θεμελιώδες ανθρώπινο δικαίωμα, σχετίζεται με την ελευθερία του ατόμου. Ωστόσο, παρόλο που υπάρχει πλήθος νομικών κειμένων που προσδιορίζουν το πλαίσιο στο οποίο πρέπει να κινείται κάθε επεξεργασία προσωπικών δεδομένων προκειμένου να μη θίγεται αυτό ακριβώς το θεμελιώδες δικαίωμα, εν τούτοις το νομικό πλαίσιο αποδεικνύεται στην πράξη ότι δεν μπορεί να συμβαδίσει πλήρως με την πρόοδο της τεχνολογίας και τους νέους κινδύνους που ανακύπτουν ακριβώς λόγω αυτής της εξέλιξης. Το Διαδίκτυο και οι εφαρμογές του αναπτύσσονται με ραγδαίους ρυθμούς στις τελευταίες δεκαετίες, εγείροντας νέους κινδύνους για την προστασία των προσωπικών δεδομένων που μέχρι πρότινος δεν υπήρχαν, και οι οποίοι στην πράξη δεν μπορούν να αντιμετωπιστούν αποτελεσματικά με τα εργαλεία που παρέχει η τεχνολογία. Οι κίνδυνοι αυτοί ουσιαστικά αυξάνονται με τις νέες δυνατότητες ταχύτατης επεξεργασίας εκατομμυρίων ψηφιακών δεδομένων μέσω ηλεκτρονικού υπολογιστή και της μεταφοράς πληροφοριών παγκοσμίως μέσω του Ιντερνέτ. Αποθήκευση και έρευνα μεγάλου όγκου δεδομένων («big data») που παλαιότερα θα απαιτούσε μεγάλους αποθηκευτικούς χώρους και επίπονη εργασία έχει πλέον απλοποιηθεί και γίνεται πολύ πιο εύκολα και ανέξοδα. Έτσι για την προστασία του ατόμου στην κοινωνία της

πληροφορίας δεν επαρκούν οι παραδοσιακές νομικές εγγυήσεις και ρυθμίσεις, αλλά χρειάζεται μια ειδική αντιμετώπιση.

Από την άλλη πλευρά, δεν πρέπει κανείς να παραβλέπει το γεγονός ότι το Διαδίκτυο αποτελεί ένα πολύτιμο εργαλείο, το οποίο μπορεί να επιλύσει διάφορα προβλήματα ή να παρέχει πολύ σημαντικές υπηρεσίες. Εξάλλου, η έννοια της διαφάνειας («open data»), ιδίως δε για θέματα που άπτονται της κρατικής δράσης, είναι επίσης ιδιαίτερα σημαντική, και πολύ συχνά προσκρούει στην απαίτηση για ιδιωτικότητα. Ως εκ τούτου, αυτό που εν τέλει απαιτείται δεν είναι η «απαγόρευση» των τεχνολογιών του Διαδικτύου προς χάριν της ιδιωτικότητας, αλλά η προσεκτική και συνετή σχεδίαση και υλοποίηση των διαδικτυακών υπηρεσιών έτσι ώστε να μη θίγεται η ιδιωτικότητα των χρηστών: αυτό ακριβώς είναι και το κύριο ζήτημα που αποτελεί την μεγαλύτερη πρόκληση τόσο από νομική αλλά, κυρίως, από τεχνολογική πλευρά.

Καταλήγοντας αναφέρουμε αυτό που είχε πει ο Φραγκλίνος Ρούσβελτ: αυτοί που θυσιάζουν την ελευθερία για την ασφάλεια δεν αξίζουν τίποτα από τα δυο. [36]

Η παρούσα διατριβή μελετά το ζήτημα της προστασίας προσωπικών δεδομένων στο Διαδίκτυο, εστιάζοντας στο υπό διαμόρφωση νέο ευρωπαϊκό νομικό πλαίσιο. Στόχος της είναι η παρουσίαση της τρέχουσας κατάστασης, ο εντοπισμός των ζητημάτων που ανακύπτουν και η κριτική μελέτη του νέου, νομικού πλαισίου, εντοπίζοντας το πώς οι επιταγές αυτού «μεταφράζονται» σε επίπεδο τεχνολογιών Διαδικτύου.

## 1.1 Η έννοια της ιδιωτικότητας

Η έννοια της ιδιωτικότητας (privacy) υπάρχει ως κοινωνικό και νομικό ζήτημα εδώ και πολλούς αιώνες, και αποτελεί μια από τις βασικές εσωτερικές ανάγκες του ανθρώπου. Η λέξη ιδιωτικότητα (privacy), προέρχεται από τη λατινική λέξη “privatus” και αναφέρεται στη προάσπιση των προσωπικών δεδομένων των χρηστών. Πάρα πολλοί ήταν οι φιλόσοφοι, και οι νομικοί που προσπάθησαν να ορίσουν τον ακριβή ορισμό της ιδιωτικότητας.

Μια πρώτη πτυχή της ιδιωτικότητας διαφαίνεται στο έργο του Αριστοτέλη όπου διαχωρίζει τον ιδιωτικό από τον δημόσιο βίο.

Κατόπιν το 1890 οι Αμερικάνοι νομικοί Samuel Warren και Louis Brandeis, με το θεμελιώδες άρθρο τους «Το δικαίωμα στην ιδιωτικότητα» (The right to privacy) [28] ορίζουν την ιδιωτικότητα ως το «Δικαίωμα να παραμένει κάποιος μόνος του (The right to be left alone)».

Έπειτα ο William Prosser, με το άρθρο του στην California Law Review, το 1960 [29], θεωρεί ότι το Αμερικάνικο δίκαιο, προστατεύει τέσσερις κατηγορίες του δικαιώματος στην ιδιωτικότητα :

1. Την παραβίαση του δικαιώματος ενός ατόμου στην μοναχικότητα ή την απομόνωση, ή την παραβίαση των προσωπικών του υποθέσεων.

2. Την δημόσια αποκάλυψη προσβλητικών ιδιωτικών γεγονότων για το άτομο.

3. Την δημοσιότητα η οποία προβάλει ψεύδη για τον δημόσιο βίο ενός ατόμου.

4. Την οικειοποίηση προς το συμφέρον τρίτου, του ονόματος, ή της υπόληψης ενός ατόμου.

Τέλος ο διαπρεπής νομικός Edward J. Bloustein, θεωρεί την ιδιωτικότητα ως μια έκφραση της ανθρώπινης αξιοπρέπειας [30].

Σύμφωνα με την κρατούσα άποψη, ο πιο αποδεκτός ορισμός της έννοιας της ιδιωτικότητας δόθηκε από τον νομικό Alan F.Westin και ορίζεται ως :

“Η αξίωση των ατόμων, των ομάδων και των ιδρυμάτων να αποφασίζουν για τον εαυτό τους πότε, πώς και σε ποιο ακριβώς βαθμό οι πληροφορίες για τα άτομά τους γνωστοποιούνται στους υπόλοιπους με τους οποίους επικοινωνούν”. [32]

Η ιδιωτικότητα πλέον κατοχυρώνεται ως ένα θεμελιώδες ανθρώπινο δικαίωμα, το οποίο το συναντάμε σε κάθε δημοκρατική κοινωνία. Η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) στο άρθρο 8 αναφέρει ότι:

[Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του]. [Χάρτης των θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης]

Επίσης, το Σύνταγμα της Ελλάδος στο άρθρο 9 αναγορεύει την κατοικία του καθενός σε άσυλο και ορίζει την ιδιωτική και οικογενειακή ζωή του ατόμου απαραβίαστη.

Αντίστοιχα, στο άρθρο 15 στο Σύνταγμα της Κυπριακής Δημοκρατίας αναφέρεται ότι "έκαστος έχει το δικαίωμα όπως η ιδιωτική και οικογενειακή αυτού ζωή τυγχάνει σεβασμού", ενώ στο άρθρο 16 αναγορεύεται την κατοικία του καθενός ως απαραβίαστη.

Συχνά οι ορισμοί της ιδιωτικότητας διαφέρουν αρκετά ο ένας από τον άλλον. Αυτό συμβαίνει γιατί, πέρα από την προσέγγιση του ορισμού από τον εκάστοτε στοχαστή, π.χ. νομική προσέγγιση, κοινωνική προσέγγιση, πολιτική προσέγγιση, για την διατύπωση ενός ορισμού παίζει σημαντικό ρόλο και το κοινωνικό-πολιτικό πλαίσιο αλλά και το περιβάλλον της εποχής στην οποία ορίζεται .

Ο Rosenberg (1992) προσέγγισε την ιδιωτικότητα ορίζοντας τρεις έννοιες [ 31 ] :

1) Χωρική – Εδαφική Ιδιωτικότητα (territorial privacy): Αναφέρεται στην προστασία του στενού φυσικού χώρου που περιβάλει ένα άτομο π.χ. χώρος εργασίας

2) Ιδιωτικότητα του ατόμου (privacy of the person): Αναφέρεται στην προστασία του ατόμου από αναίτιες παρεμβάσεις τρίτων σε αυτό, π.χ. φυσική έρευνα χωρίς δικαιολογία, έλεγχο για κατοχή φαρμάκων, ανήθικη και παράνομη έρευνα για την απόκτηση προσωπικών πληροφοριών κλπ.

3) Ιδιωτικότητα της πληροφορίας (informational privacy): Αναφέρεται στο ειδικότερο δικαίωμα του κάθε ατόμου να ελέγχει αν και με ποιο τρόπο τα προσωπικά του δεδομένα συλλέγονται, αποθηκεύονται επεξεργάζονται και διαμοιράζονται σε τρίτους.

Παρ' όλες όμως τις εναλλαγές το δικαίωμα στην ιδιωτικότητα δεν διαφοροποιείται ουσιωδώς. Ωστόσο, με την πάροδο των ετών και με την αλματώδη εξέλιξη της τεχνολογίας, έχουν αλλάξει δραματικά οι τεχνικές δυνατότητες παραβίασής του.

## 1.2 Η Ιδιωτικότητα σε περιβάλλον διαδικτύου

Η διάδοση της τεχνολογίας των υπολογιστών πλέον είναι κυρίαρχη σε όλους τους τομείς της ζωή μας , ενώ η διασύνδεση των υπολογιστών μέσω του διαδικτύου έχει επιφέρει δραματική αλλαγή στην οικονομική και στην κοινωνική ανάπτυξη της κοινωνίας. Έτσι η συλλογή πληροφοριών καθίσταται ιδιαίτερα εύκολη στην σημερινή εποχή, όπου καθημερινά δεκάδες χιλιάδες δεδομένα μεταφέρονται μέσα από διεθνή δίκτυα μέσα σε ελάχιστο χρόνο , δια μέσου του διαδικτύου.

Ωστόσο τα νέα συστήματα της τεχνολογίας και οι νέες εφαρμογές έχουν καταστήσει και ιδιαίτερα δυσχερή την εφαρμογή της νομοθεσίας περί προστασίας των προσωπικών δεδομένων. Σημαντικά ζητήματα για την προστασία των προσωπικών δεδομένων προκύπτουν, από τα διάφορα λογισμικά συστήματα και εφαρμογές του κυβερνοχώρου. Καθώς ολοένα και περισσότερες εφαρμογές χρησιμοποιούν προσωπικά δεδομένα, π.χ. για την παροχή νέων, προσωποποιημένων υπηρεσιών, που διευκολύνουν το χρήστη στις καθημερινές του συναλλαγές με τον ψηφιακό κόσμο. Ταυτόχρονα όμως, παρουσιάζονται συνεχώς και νέοι κίνδυνοι, τόσο αναφορικά με την αθέλητη αποκάλυψη της ταυτότητας των χρηστών, όσο και με την παραβίαση της επεξεργασίας των προσωπικών τους δεδομένων. Για όλους αυτούς τους λόγους είναι πλέον επιτακτική η ανάγκη δημιουργίας νομικών κανόνων ικανών να προστατεύουν επαρκώς την ιδιωτική ζωή του ατόμου, αλλά και κυρίως μηχανισμών εφαρμογής τους οι οποίοι θα πρέπει να βρίσκονται σε συνεχή εναρμόνιση με τις σύγχρονες τεχνολογικές εξελίξεις.

Έτσι, στην σύγχρονη ψηφιακή εποχή όπου ζούμε, προβάλει έντονα η ανάγκη για τον εκσυγχρονισμό του νομικού πλαισίου και την θέσπιση νέου που θα είναι αναπόσπαστα συνδεδεμένο με τις τεχνολογικές εξελίξεις, και το οποίο θα μπορεί να εξασφαλίσει επαρκή προστασία έναντι τον διαφαινόμενων απειλών. Προς αυτήν την κατεύθυνση κινείται το σχέδιο του νέου κανονισμού της Ευρωπαϊκής Ένωσης για την προστασία των προσωπικών δεδομένων.

## 1.3 Δομή της διατριβής

Η παρούσα διατριβή αποτελεί μια μελέτη των βασικών αρχών προστασίας προσωπικών δεδομένων , όπως αυτές ισχύουν μέχρι σήμερα , καθώς και της νέας πρότασης Κανονισμού της Ευρωπαϊκής Επιτροπής που είναι υπό διαβούλευση .

Στο πρώτο κεφάλαιο επισημαίνεται η έννοια της ιδιωτικότητας, η οποία είναι άρρηκτα συνδεδεμένη με τα προσωπικά δεδομένα των ανθρώπων ,

Στο δεύτερο κεφάλαιο αναλύεται ο ορισμός των προσωπικών δεδομένων, τονίζεται η ανάγκη για την προστασία τους , και γίνεται αναφορά στο το υπάρχον νομικό πλαίσιο .

Στο τρίτο κεφάλαιο αναφέρονται κύρια τεχνολογικά θέματα που βάζουν σε κίνδυνο την προστασία των προσωπικών δεδομένων στο διαδίκτυο ,

Στο τέταρτο κεφάλαιο αναλύεται ο νέος κανονισμός της Ευρωπαϊκής Ένωσης ο οποίος είναι υπό διαβούλευση, και τονίζεται η αναγκαιότητα αυτής της αλλαγής στον τομέα της πληροφορικής.

Και στο τελευταίο κεφάλαιο επισημαίνονται τα προβλήματα που πιθανότατα να προκύψουν κατά την εφαρμογή του νέου κανονισμού με βάση της υπάρχουσα τεχνολογίας.

# Κεφάλαιο 2
# Η προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση

Όπως ήδη αναφέρθηκε στο προηγούμενο κεφάλαιο, η ανάγκη για την κατοχύρωση του σεβασμού και της προστασίας της ανθρώπινης αξιοπρέπειας, της ιδιωτικής ζωής και της ελεύθερης ανάπτυξης της προσωπικότητας του ατόμου (και κατ' επέκταση της ασφάλειας των προσωπικών δεδομένων του, ως μιας έκφανση του δικαιώματος της ανθρώπινης αξιοπρέπειας) θεωρούνται θεμελιώδη δικαιώματα και κατευθυντήριες αρχές κάθε δημοκρατικής κοινωνίας. Ως εκ τούτου, η προστασία των προσωπικών δεδομένων, αποτελεί μια ιδιαίτερα σημαντική πτυχή της ιδιωτικότητας των ατόμων.

Η προσπάθεια για την τήρηση των ανωτέρω αρχών δεν είναι εύκολη. Το πρόβλημα δε επιτείνεται από την τεράστια πρόοδο στον τομέα της πληροφορικής, την ανάπτυξη νέων ισχυρών τεχνολογιών, νέων μορφών ηλεκτρονικών συναλλαγών και των αναγκών για την ηλεκτρονική οργάνωση του κράτους (ηλεκτρονική διακυβέρνηση), τα οποία συντελούν στο να υπάρχει αυξημένη ζήτηση των προσωπικών πληροφοριών από τους ιδιωτικούς και τους δημόσιους φορείς.

Κύριο στόχο, σε ευρωπαϊκό επίπεδο, αποτέλεσε η προστασία της ιδιωτικής ζωής, και κατ' επέκταση η προστασία των προσωπικών δεδομένων των πολιτών, ταυτόχρονα όμως με την διευκόλυνση της νόμιμης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα εντός της Ευρωπαϊκής Ένωσης. Στο κεφάλαιο αυτό θα περιγράψουμε το υπάρχον νομικό πλαίσιο της Ευρωπαϊκής Ένωσης που κατοχυρώνει την προστασία των προσωπικών δεδομένων .

## 2.1 Νομικό Πλαίσιο

Για την προστασία των προσωπικών δεδομένων του ατόμου στην σύγχρονη εποχή κρίθηκε ότι χρειάζεται μια νομική ρύθμιση η οποία θα ρυθμίσει ενιαία το ζήτημα στην Ευρωπαϊκή Ένωση, καθώς δεν θεωρείται ότι δεν επαρκούν οι νομικές ρυθμίσεις και εγγυήσεις σε επίπεδο κρατών. Στο πλαίσιο αυτό έχει θεσπιστεί η ευρωπαϊκή οδηγία 95/46/ΕΚ η οποία αποτελεί το βασικό κείμενο αναφοράς σε ευρωπαϊκό επίπεδο για θέματα προστασίας δεδομένων προσωπικού χαρακτήρα.

Η οδηγία αυτή θέτει τους κατευθυντήριους κανόνες για την προστασία των προσωπικών δεδομένων σε όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης.

Με την οδηγία αυτή θεσπίζεται ένα κανονιστικό πλαίσιο που αποσκοπεί στην εγκαθίδρυση μιας ισορροπίας μεταξύ του υψηλού επιπέδου προστασίας της ιδιωτικής ζωής των προσώπων και της διευκόλυνσης της νόμιμης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα ανά την Ευρωπαϊκή Ένωση (ΕΕ). Προς το σκοπό αυτό, η οδηγία ορίζει τα όρια για τη συλλογή και τη χρησιμοποίηση των δεδομένων προσωπικού χαρακτήρα και απαιτεί τη δημιουργία, σε κάθε κράτος μέλος, ενός ανεξάρτητου εθνικού φορέα επιφορτισμένου με την προστασία των δεδομένων αυτών.

Σε όλα τα κράτη-μέλη έχει ενσωματωθεί η ανωτέρω οδηγία στην εθνική τους έννομη τάξη (με μικρές διαφοροποιήσεις σε επί μέρους σημεία – ο «πυρήνας» της οδηγίας είναι κοινός σε όλες τις χώρες). Επίσης, σε όλα τα κράτη-μέλη έχει θεσπιστεί μια ανεξάρτητη Αρχή, με κύρια αποστολή την εποπτεία εφαρμογής του σχετικού νόμου περί προστασίας προσωπικών δεδομένων.

Στην Κύπρο υπάρχει το Γραφείο Επιτρόπου Προστασίας Δεδομένων το οποίο συστάθηκε το Μάιο 2002 μετά τη θέσπιση του περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα

(Προστασία του Ατόμου) Νόμου του 2001. Ο Νόμος εφαρμόζεται τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα, συμπεριλαμβανομένης της Αστυνομίας. Ο Νόμος προβλέπει τον διορισμό Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για περίοδο 4 χρόνων, η οποία μπορεί να ανανεωθεί για ακόμα μια περαιτέρω θητεία. Σήμερα επίτροπος είναι κ. Γιάννος Δανιηλίδης ο οποίος ανέλαβε τα καθήκοντα του στις 27.9.2011.

Στην Ελλάδα αντίστοιχα, υπάρχει η Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΔΠΧ), η οποία είναι μια ανεξάρτητη διοικητική Αρχή, η οποία λειτουργεί από τον Νοέμβριο του 1997. Η ίδρυση της έγινε με τον Νόμο 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα (ο οποίος ενσωματώνει στο ελληνικό Δίκαιο την οδηγία 95/46/ΕΚ), και δρα ως ανεξάρτητη διοικητική αρχή, δηλαδή μη υπαγόμενη σε κανενός είδους έλεγχο από την κυβέρνηση. Σημειώνεται ότι η ΑΠΔΠΧ είναι και συνταγματικά κατοχυρωμένη στο άρθρο 9Α του Συντάγματος. Άλλες αρχές που εποπτεύουν την επεξεργασία προσωπικών δεδομένων είναι στην Ελλάδα η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών και στην Ευρώπη ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων.

Δεδομένου ότι όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης έχουν ουσιαστικά τις ίδιες αρχές όσον αφορά το νομικό πλαίσιο προστασίας προσωπικών δεδομένων, στη συνέχεια του κεφαλαίου παρατίθενται οι αρχές αυτές, ακολουθούμενες από χαρακτηριστικά παραδείγματα προς αποσαφήνισή τους,

## 2.2 Τι είναι τα προσωπικά δεδομένα

Δεδομένα προσωπικού χαρακτήρα (ή αλλιώς ***προσωπικά δεδομένα)*** αποτελούν οποιεσδήποτε πληροφορίες αναφέρονται και περιγράφουν ένα άτομο, του οποίου η ταυτότητά του είναι γνωστή **ή μπορεί να εξακριβωθεί**, άμεσα ή έμμεσα. Για παράδειγμα, αυτές οι πληροφορίες μπορεί να είναι :

- τα στοιχεία αναγνώρισης (ονοματεπώνυμο, αριθμός δελτίου ταυτότητας, αριθμός φορολογικού μητρώου κλπ.)
- ιδιότητες (ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.)
- τα φυσικά χαρακτηριστικά του ατόμου

- η εκπαίδευσή του ,
- η εργασία του (προϋπηρεσία, εργασιακή συμπεριφορά κλπ)
- η οικονομική του κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά),
- τα ενδιαφέροντά του
- άλλες δραστηριότητές του
- κάθε είδους αρχείο που αναφέρεται στο άτομο (φωτογραφία, ήχος κτλ.)
- οι συνήθειές του

Εδώ θα πρέπει να σημειώσουμε ότι η έννοια των προσωπικών δεδομένων είναι πολύ πιο ευρεία από ότι ίσως μπορεί κανείς να αναλογιστεί: και αυτό απορρέει από τον ανωτέρω ορισμό, που ως προσωπικό δεδομένο εκλαμβάνεται και οτιδήποτε δύναται να συντελέσει στην ταυτοποίηση του χρήστη. Ως ενδεικτικό παράδειγμα, σημειώνεται ότι και στην περίπτωση μιας υπηρεσίας κοινωνικής δικτύωσης που δεν έχουμε δώσει το πραγματικό μας όνομα αλλά ένα ψευδώνυμο (nickname), αυτό επίσης εμπίπτει στη έννοια των προσωπικών δεδομένων, καθώς μπορεί να συντελέσει (ενδεχομένως σε συνδυασμό με άλλες πληροφορίες) στην πλήρη ταυτοποίηση του χρήστη. Αντίστοιχα, και η διαδικτυακή (IP) διεύθυνση του υπολογιστή, εκλαμβάνεται ως προσωπικό δεδομένο, γιατί μπορεί επίσης, έστω και υπό προϋποθέσεις, να αποκαλύψει τον χρήστη του υπολογιστή.

Υπάρχουν όμως και κάποιες ιδιαίτερες κατηγορίες προσωπικών δεδομένων, τα λεγόμενα **ευαίσθητα προσωπικά δεδομένα,** τα οποία χρήζουν ακόμα μεγαλύτερης προστασίας λόγω του ότι εμπίπτουν στον λεγόμενο σκληρό πυρήνα του δικαιώματος της ιδιωτικότητας.

Τα δεδομένα αυτά είναι εκείνα τα οποία αναφέρονται:

- στη φυλετική ή εθνική προέλευση,
- στα πολιτικά φρονήματα,
- στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις,
- στη συμμετοχή σε συνδικαλιστική οργάνωση,
- στην υγεία,

- στην κοινωνική πρόνοια,
- στην ερωτική ζωή του ατόμου,
- στις ποινικές διώξεις και καταδίκες
- καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

Τα ευαίσθητα δεδομένα προστατεύονται από τον νόμο (όπως θα δούμε στη συνέχεια) με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα. Στην πράξη, τα μη ευαίσθητα προσωπικά δεδομένα είθισται να αποκαλούνται απλά προσωπικά δεδομένα.

Επισημαίνεται ότι συγκεντρωτικά δεδομένα στατιστικής φύσης, από τα οποία δεν μπορεί να εξαχθεί κάποια πληροφορία σχετικά με τα άτομα στα οποία αναφέρονται, δεν αποτελούν δεδομένα προσωπικού χαρακτήρα: σε αυτές τις περιπτώσεις, δεν εφαρμόζεται το εν λόγω νομικό πλαίσιο.

## 2.3 Επεξεργασία των προσωπικών δεδομένων

**Υποκείμενο των δεδομένων** ορίζεται το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται οι πληροφορίες των προσωπικών δεδομένων .

Επεξεργασία των προσωπικών δεδομένων αποκαλείται οποιαδήποτε ενέργεια, η οποία αφορά τα δεδομένα προσωπικού χαρακτήρα όπως: συλλογή, καταχώρηση, οργάνωση, διατήρηση ή αποθήκευση, εξαγωγή, χρήση, ανάγνωση, διαβίβαση, διάδοση, συσχέτιση, τροποποίηση, δέσμευση , διασύνδεση, καταστροφή ή διαγραφή.

Από το ανωτέρω ορισμό γίνεται σαφές ότι, πρακτικά, οποιαδήποτε ενέργεια επί προσωπικών δεδομένων αποτελεί επεξεργασία αυτών και, ως εκ τούτου, υπόκειται στο σχετικό νόμο. Καθημερινά υπάρχουν γύρω μας αμέτρητα παραδείγματα επεξεργασίας **προσωπικών δεδομένων**:

- Οι ιατροί τηρούν αρχεία ιατρικών εξετάσεών μας, αλλά και άλλα σχετικά με την υγεία μας στοιχεία. Περαιτέρω, κάθε συνταγογράφηση γίνεται πλέον ηλεκτρονικά, οπότε

υπάρχει δημιουργία κεντρικού αρχείου με τις συνταγογραφήσεις όλων των ασθενών. Τα ανωτέρω αποτελούν επεξεργασία ευαίσθητων προσωπικών δεδομένων (δεδομένων υγείας).

- Η Γενική Γραμματεία Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών τηρεί τα φορολογικά στοιχεία όλων φορολογουμένων (απλά προσωπικά δεδομένα)
- Οι εργοδότες τηρούν στοιχεία υπαλλήλων (βιογραφικά σημειώματα, τίτλους, αναρρωτικές άδειες κτλ – απλά αλλά και ευαίσθητα προσωπικά δεδομένα)
- Κατά την εγγραφή ενός χρήστη σε μία διαδικτυακή υπηρεσία, συμπληρώνει διάφορα στοιχεία τα οποία και τηρούνται από τον πάροχο της υπηρεσίας
- Σε μία υπηρεσία κοινωνικής δικτύωσης, αναρτούμε οι ίδιοι προσωπικά μας δεδομένα (φωτογραφίες, απόψεις μας, δήλωση φίλων μας).
- Όταν κάποιος «σερφάρει» στο Διαδίκτυο, οι προτιμήσεις του στις σελίδες που επισκέπτεται καταγράφονται με σκοπό την εμφάνιση στον υπολογιστή του αντίστοιχων διαφημιστικών μηνυμάτων.

Όλα τα παραπάνω είναι μία ενδεικτική λίστα των διαφόρων ειδών επεξεργασίας που υφίστανται τα προσωπικά μας δεδομένα, ενώ υπάρχουν ακόμα εκατοντάδες τέτοιες λίστες που θα μπορούσε να καταγράψει κανείς με βάση την καθημερινότητα ενός ατόμου .

Οοποιοδήποτε φυσικό ή νομικό πρόσωπο του δημοσίου ή ιδιωτικού τομέα καθορίζει το σκοπό και τον τρόπο της επεξεργασίας ονομάζεται **υπεύθυνος επεξεργασίας** και είναι αυτός που έχει την κύρια ευθύνη όσο αφορά την πλήρη εξασφάλιση της ασφάλειας των προσωπικών δεδομένων και τη γενικότερη συμμόρφωση με τις διατάξεις του νόμου περί προστασίας προσωπικών δεδομένων. Αντίστοιχα κάθε φυσικό ή νομικό πρόσωπο του δημόσιου ή ιδιωτικού τομέα που επεξεργάζεται δεδομένα για λογαριασμό κάποιου υπεύθυνου επεξεργασίας ονομάζεται **εκτελών την επεξεργασία.** Για παράδειγμα, αν ένας δημόσιος οργανισμός έχει αναθέσει σε μία επιχείρηση την ανάπτυξη και συντήρηση πληροφοριακού συστήματος, μέσω του οποίου πραγματοποιείται επεξεργασία προσωπικών δεδομένων, τότε ο οργανισμός αποτελεί τον υπεύθυνο επεξεργασίας, ενώ η επιχείρηση αποτελεί τον εκτελούντα την επεξεργασία.

Επίσης η Ευρωπαϊκή Οδηγία 95/46 στα άρθρα 26 και 27 [61] ενθαρρύνει τα κράτη και τους υπεύθυνους επεξεργασίας να καταρτίσουν κώδικες δεοντολογίας βάση των οποίων θα γίνεται η

οποιαδήποτε επεξεργασία των δεδομένων, οι δεοντολογικοί κώδικες υποβάλλονται στην νομική αρχή του κάθε κράτους μαζί με την σύσταση λειτουργίας αρχείου προσωπικών δεδομένων, όπου μέσα θα αναφέρεται αναλυτικά ο σκοπός της συλλογής και επεξεργασίας των προσωπικών δεδομένων η οποία αρχή μπορεί να τους δημοσιεύει καταλλήλως.

Οποιαδήποτε μη συμμόρφωση των υπεύθυνων επεξεργασίας στην διαχείριση των προσωπικών δεδομένων αποτελεί διάπραξη πειθαρχικού παραπτώματος και διώκεται νομικά**.**

## 2.4 Προϋποθέσεις νομιμότητας της επεξεργασίας των προσωπικών δεδομένων

Θεμελιώδεις προϋποθέσεις για τη νομιμότητα της επεξεργασίας προσωπικών δεδομένων αποτελούν η αρχή του σκοπού και η αρχή της αναλογικότητας. Ειδικότερα, για να είναι νόμιμη η επεξεργασία προσωπικών δεδομένων, θα πρέπει:

- Τα δεδομένα να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς, και να υφίστανται επεξεργασία μόνο στο πλαίσιο των σκοπών αυτών (αρχή του σκοπού)
- Να είναι συναφή, πρόσφορα και όχι περισσότερα από όσα κάθε φορά απαιτείται για το σκοπό επεξεργασίας (αρχή της αναλογικότητας)
- Να είναι ακριβή και μόνο όσα απαιτεί ο σκοπός της επεξεργασίας
- Να επιτρέπουν τον προσδιορισμό της ταυτότητας του υποκειμένου μόνο κατά την διάρκεια που απαιτείται για την ολοκλήρωση των σκοπών της συλλογής τους και την επεξεργασία τους. Με την παρέλευση της περιόδου αυτής τα δεδομένα πρέπει να καταστρέφονται.

Ιδιαίτερα η αρχή της αναλογικότητας είναι ιδιαίτερα σημαντική, αφού καλύπτει κρίσιμα τμήματα της επεξεργασίας τα οποία, σε πολλές περιπτώσεις, είναι δυσδιάκριτα: γενικότερα, βάσει της αρχής της αναλογικότητας, προκύπτει ότι τα συλλεγόμενα στοιχεία πρέπει να είναι αναγκαία και πρόσφορα για τον επιδιωκόμενο σκοπό, ο οποίος δεν μπορεί να επιτευχθεί με εξίσου αποτελεσματικά αλλά λιγότερο επαχθή μέσα. Το ανωτέρω είναι ζωτικής σημασίας για την προστασία των ατόμων, ωστόσο το ερώτημα δεν έχει πάντα προφανή απάντηση «είναι πράγματι υποχρεωτικό να συλλέγουν όλα τα δεδομένα που μου ζητούνται;» δεν έχει πάντα προφανή απάντηση.

Επισημαίνεται ότι εφόσον για δεδομένα που έχουν συλλεχθεί διαπιστωθεί κατά την επεξεργασία τους ότι υπάρχει νομική παράβαση , θα πρέπει να γίνεται αυτομάτως διακοπή της συλλογής ή της επεξεργασίας και τα προσωπικά δεδομένα να καταστρέφονται με πλήρη ευθύνη του υπευθύνου επεξεργασίας των δεδομένων.

Πέραν των ανωτέρω, βασική προϋπόθεση για τη νομιμότητα της επεξεργασίας είναι η σαφής, ρητή και ειδική συγκατάθεση των υποκειμένων των δεδομένων. Υπάρχουν περιπτώσεις όπου η επεξεργασία μπορεί να είναι νόμιμη και χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων (για παράδειγμα, όταν επιβάλλεται από νόμο, όταν είναι αναγκαία για την εκτέλεση σύμβασης, ή όταν η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση έννομου συμφέροντος του υπευθύνου επεξεργασίας ή τρίτου και το οποίο υπερέχει προφανώς των δικαιωμάτων των προσώπων στα οποία αναφέρονται τα δεδομένα).

## 2.5 Υποχρέωση για γνωστοποίηση και ασφάλεια της επεξεργασίας

Το άρθρο 6 του Ν2472/1997 αναφέρει ότι ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή , τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας .

Με την γνωστοποίηση αυτή πρέπει να δηλώσει τα προσωπικά του δεδομένα (ονοματεπώνυμο ή επωνυμία ή τίτλος) καθώς και την διεύθυνση όπου είναι εγκατεστημένο το αρχείο ή ο κύριος εξοπλισμός που υποστηρίζει την επεξεργασία των δεδομένων .

Επιπλέον θα γίνει αναλυτική περιγραφή :

- στο σκοπού της επεξεργασίας ,
- στο είδος των δεδομένων
- στο χρονικό διάστημα όπου θα πραγματοποιηθεί η όποια επεξεργασία
- στους αποδέκτες όπου θα ανακοινωθούν τα προσωπικά δεδομένα
- στις όποιες διαβιβάσεις ενδεχομένως να γίνουν σε τρίτες χώρες
- στα βασικά χαρακτηριστικά του συστήματος και στα μέτρα ασφαλείας του συστήματος

Το άρθρο10 του Ν2472/1997 τονίζει ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι πάντα απόρρητη .
Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία, και μόνον κατ' εντολή του.
Επιπλέον ο υπεύθυνος επεξεργασίας οφείλει να λάβει όλα τα απαραίτητα μέτρα για την αυστηρή τήρηση του απορρήτου και την πλήρη προστασία των δεδομένων από οποιονδήποτε κίνδυνο , και κυρίως από κάθε είδους αθέμιτη επεξεργασία .
Και τέλος η αρχή παρέχει οδηγίες ή εκδίδει κανονιστικές πράξεις σχετικά με τον βαθμό ασφάλειας των δεδομένων και των υπολογιστικών και επικοινωνιακών υποδομών, καθώς και για τη χρήση τεχνολογιών ενίσχυσης της ιδιωτικότητας.

## 2.6 Επεξεργασία ευαίσθητων δεδομένων

Στο άρθρο 7 του ν 2472 αναφέρεται ότι στα ευαίσθητα προσωπικά δεδομένα, απαγορεύεται η συλλογή και η επεξεργασία των ευαίσθητων δεδομένων.

Ωστόσο κατ' εξαίρεση επιτρέπεται η συλλογή και η επεξεργασία τους , καθώς και η ίδρυση και λειτουργία σχετικού αρχείου, μόνο ύστερα από άδεια της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, και μόνο όταν συντρέχουν μία ή περισσότερες από τις ακόλουθες προϋποθέσεις:

- Το υποκείμενο έδωσε τη γραπτή συγκατάθεσή του, εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που αντίκειται στο νόμο ή τα χρηστά ήθη.

- Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

- Η επεξεργασία αφορά δεδομένα που δημοσιοποιεί το ίδιο το υποκείμενο ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου ή πειθαρχικού οργάνου.

- Η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που ασχολείται κατ' επάγγελμα με την παροχή υπηρεσιών υγείας και υπόκειται σε καθήκον εχεμύθειας ή σε συναφείς κώδικες δεοντολογίας, υπό τον όρο ότι η επεξεργασία είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας.

- Η επεξεργασία εκτελείται από Δημόσια Αρχή και είναι αναγκαία είτε για λόγους εθνικής ασφάλειας, είτε για την εξυπηρέτηση των αναγκών εγκληματολογικής ή σωφρονιστικής πολιτικής και αφορά τη διακρίβωση εγκλημάτων, ποινικές καταδίκες ή μέτρα ασφαλείας είτε για λόγους προστασίας της δημόσιας υγείας, είτε για την άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών.

- Η επεξεργασία πραγματοποιείται για ερευνητικούς και επιστημονικούς αποκλειστικά σκοπούς και υπό τον όρο ότι τηρείται η ανωνυμία και λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται.

- Η επεξεργασία αφορά δεδομένα δημοσίων προσώπων, εφόσον αυτά συνδέονται με την άσκηση δημοσίου λειτουργήματος ή τη διαχείριση συμφερόντων τρίτων, και πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος. Η άδεια της Αρχής χορηγείται μόνο εφόσον η επεξεργασία είναι απολύτως αναγκαία για την εξασφάλιση του δικαιώματος πληροφόρησης επί θεμάτων δημοσίου ενδιαφέροντος καθώς και στο πλαίσιο καλλιτεχνικής έκφρασης και εφόσον δεν παραβιάζεται με οποιονδήποτε τρόπο το δικαίωμα προστασίας της ιδιωτικής και οικογενειακής ζωής.

Η Αρχή χορηγεί άδεια συλλογής και επεξεργασίας ευαίσθητων δεδομένων, καθώς και άδεια ιδρύσεως και λειτουργίας σχετικού αρχείου, ύστερα από αίτηση του υπεύθυνου επεξεργασίας. Εφόσον η Αρχή διαπιστώσει ότι πραγματοποιείται επεξεργασία ευαίσθητων δεδομένων, η γνωστοποίηση αρχείου επέχει θέση αιτήσεως για τη χορήγηση άδειας.

Η Αρχή μπορεί να επιβάλλει όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων. Πριν χορηγήσει την άδεια, η Αρχή καλεί σε ακρόαση τον υπεύθυνο επεξεργασίας ή τον εκπρόσωπο του και τον εκτελούντα την επεξεργασία.

Η άδεια εκδίδεται για ορισμένο χρόνο, ανάλογα με τον σκοπό της επεξεργασίας. Και μπορεί να ανανεωθεί ύστερα από αίτηση του υπεύθυνου επεξεργασίας.

Υπάρχουν όμως και μερικές περιπτώσεις όπου οι υπεύθυνοι επεξεργασίας απαλλάσσονται από την υποχρέωση γνωστοποίησης και λήψης άδειας και αυτές είναι :

1. Όταν η επεξεργασία πραγματοποιείται για σκοπούς που συνδέονται άμεσα με τη σχέση εργασίας ή έργου και είναι αναγκαία για την εκπλήρωση υποχρέωσης που επιβάλλει ο νόμος ή για την εκτέλεση της σύμβασης και το υποκείμενο των δεδομένων έχει προηγουμένως ενημερωθεί πλήρως, και δώσει την εκ των προτέρων έγκυρη και ισχυρή συγκατάθεση του.

2. Όταν η επεξεργασία αφορά πελάτες ή προμηθευτές, του υποκειμένου των δεδομένων εφόσον τα δεδομένα δε διαβιβάζονται ούτε κοινοποιούνται σε τρίτους.

3. Τα δικαστήρια και οι δημόσιες αρχές δεν λογίζονται ως τρίτοι, εφόσον τη διαβίβαση ή κοινοποίηση επιβάλλει νόμος ή δικαστική απόφαση.

4. Δεν απαλλάσσονται από την υποχρέωση γνωστοποίησης οι ασφαλιστικές εταιρείες για όλους τους κλάδους ασφάλισης, οι φαρμακευτικές εταιρείες εμπορίας πληροφοριών και τα χρηματοπιστωτικά ιδρύματα, όπως οι τράπεζες και οι εταιρείες έκδοσης πιστωτικών καρτών.

5. Όταν η επεξεργασία γίνεται από ίδρυμα, σωματείο, εταιρεία ή πολιτικά κόμματα και αφορά δεδομένα των μελών τους, εφόσον τα μέλη αυτά έχουν δώσει τη συγκατάθεσή τους και τα δεδομένα δε διαβιβάζονται ούτε κοινοποιούνται σε τρίτους. Δε λογίζονται τρίτοι τα μέλη εφόσον η διαβίβαση γίνεται προς αυτούς για τους σκοπούς των πιο πάνω

ιδρυμάτων, σωματείων, εταιρειών ή πολιτικών κομμάτων, ούτε τα δικαστήρια και οι δημόσιες αρχές, εφόσον τη διαβίβαση επιβάλλει νόμος ή δικαστική απόφαση.

6. Όταν η επεξεργασία γίνεται από ιατρούς ή άλλα πρόσωπα που παρέχουν υπηρεσίες υγείας και αφορά ιατρικά δεδομένα, εφόσον ο υπεύθυνος επεξεργασίας δεσμεύεται από το ιατρικό απόρρητο ή άλλο απόρρητο που προβλέπει νόμος ή κώδικας δεοντολογίας και τα δεδομένα δε διαβιβάζονται ούτε κοινοποιούνται σε τρίτους. Δεν εμπίπτουν στην απαλλαγή της παρούσας διάταξης τα πρόσωπα που παρέχουν υπηρεσίες υγείας, όπως κλινικές, νοσοκομεία, κέντρα υγείας, κέντρα αποθεραπείας και αποτοξίνωσης, ασφαλιστικά ταμεία και ασφαλιστικές εταιρείες, καθώς και οι υπεύθυνοι επεξεργασίας δεδομένων προσωπικού χαρακτήρα όταν η επεξεργασία διεξάγεται στο πλαίσιο προγραμμάτων τηλεϊατρικής ή παροχής ιατρικών υπηρεσιών μέσω δικτύου.

7. Όταν η επεξεργασία γίνεται από δικηγόρους και αφορά την παροχή νομικών υπηρεσιών προς πελάτες τους, εφόσον ο υπεύθυνος επεξεργασίας δεσμεύεται από υποχρέωση απορρήτου που προβλέπει νόμος και τα δεδομένα δε διαβιβάζονται ούτε κοινοποιούνται σε τρίτους, εκτός από τις περιπτώσεις που αυτό είναι αναγκαίο και συνδέεται άμεσα με την εκπλήρωση εντολής του πελάτη.

## 2.7 Τα δικαιώματα των υποκειμένων των δεδομένων

Ο Νόμος 2472/1997 σας δίνει σημαντικά δικαιώματα έναντι όλων όσων τηρούν και επεξεργάζονται τα προσωπικά σας δεδομένα. Τα δικαιώματα αυτά είναι:

**Το άρθρο 11 του νόμου 2472 αναφέρει το δικαίωμα της ενημέρωσης :**

Ο υπεύθυνος επεξεργασίας οφείλει, κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με τρόπο πρόσφορο και σαφή το υποκείμενο για τα εξής τουλάχιστον στοιχεία:

1. την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του
2. τον σκοπό της επεξεργασίας.
3. τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων.
4. την ύπαρξη του δικαιώματος πρόσβασης

**Το άρθρο 12 του νόμου 2472 αναφέρει το δικαίωμα της πρόσβασης :**

Με αυτό το άρθρο το υποκείμενο των δεδομένων ότι έχει το δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας, χωρίς καθυστέρηση και κατά τρόπο εύληπτο και σαφή, τις ακόλουθες πληροφορίες:

1. Όλα τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, καθώς και την προέλευσή τους.
2. Τους σκοπούς της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών.
3. Την εξέλιξη της επεξεργασίας για το χρονικό διάστημα από την προηγούμενη ενημέρωση ή πληροφόρησή του.
4. Τη λογική της αυτοματοποιημένης επεξεργασίας.
5. Κατά περίπτωση, τη διόρθωση, τη διαγραφή ή τη δέσμευση (κλείδωμα) των δεδομένων των οποίων η επεξεργασία δεν είναι σύμφωνη προς τις διατάξεις του παρόντος νόμου, ιδίως λόγω του ελλιπούς ή ανακριβούς χαρακτήρα των δεδομένων, και
6. Την κοινοποίηση σε τρίτους, στους οποίους έχουν ανακοινωθεί τα δεδομένα, κάθε διόρθωσης, διαγραφής ή δέσμευσης (κλειδώματος) που διενεργείται, εφόσον τούτο δεν είναι αδύνατον ή δεν προϋποθέτει δυσανάλογες προσπάθειες.

Ο υπεύθυνος επεξεργασίας οφείλει να σας απαντήσει εγγράφως εντός δεκαπέντε (15) ημερών. Σε περίπτωση που ο υπεύθυνος επεξεργασίας δεν απαντήσει εντός των δεκαπέντε (15) ημερών ή εάν η απάντηση του δεν είναι ικανοποιητική, τότε μπορεί το υποκείμενο των δεδομένων να υποβάλει αναφορά/καταγγελία στην Αρχή και να ζητήσει εξετάσει το αίτημα σας.

**Το άρθρο 13 του νόμου 2472 αναφέρει το δικαίωμα της αντίρρησης:**

Το υποκείμενο των δεδομένων έχει δικαίωμα να προβάλλει οποτεδήποτε αντιρρήσεις με μια έγγραφη συστημένη επιστολή σας προς στον υπεύθυνο επεξεργασίας και να ζητήσει την διόρθωση ή διαγραφή των προσωπικών του δεδομένων

Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να απαντήσει εγγράφως επί των αντιρρήσεων μέσα σε αποκλειστική προθεσμία δεκαπέντε ημερών. Στην απάντησή του οφείλει να ενημερώσει το υποκείμενο για τις ενέργειες στις οποίες προέβη ή, ενδεχομένως, για τους λόγους που δεν ικανοποίησε το αίτημα.

Σε περίπτωση όπου ο υπεύθυνος επεξεργασίας δεν απαντήσει εντός των 15 ημερών ή σε περίπτωση απόρριψης των αντιρρήσεων ,τότε το υποκείμενο των δεδομένων μπορεί να κάνει κοινοποιήσει / καταγγελία στην Αρχή και να ζητήσει την εξέταση του αιτήματος του.

# Κεφάλαιο 3
# Τεχνολογικά θέματα προστασίας προσωπικών δεδομένων

Με την ραγδαία πρόοδο της τεχνολογίας και των νέων εφαρμογών, η εφαρμογή πολλών εκ των επιταγών της νομοθεσίας περί προστασίας των προσωπικών δεδομένων καθίσταται ιδιαίτερα δυσχερής. Θέματα καίριας σημασίας για την προστασία των προσωπικών δεδομένων συχνά «παρακάμπτονται» από τα διάφορα συστήματα / εφαρμογές , ο κάθε χρήστης του διαδικτύου οφείλει να είναι όσο τον δυνατόν περισσότερο ενημερωμένος, για να μπορεί να διακρίνει και να αποφύγει τους κινδύνους που κρύβει το διαδίκτυο.

## 3.1 Cookies

Ένα από τα βασικά θέματα που είναι άμεσης προτεραιότητας ως προς την προστασία των προσωπικών δεδομένων στο Διαδίκτυο, είναι η δημιουργία προφίλ των χρηστών (profiling). Με τον όρο «δημιουργία προφίλ» αναφερόμαστε γενικότερα σε οποιαδήποτε αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, η οποία αποσκοπεί στο να αναλύεται ή να προβλέπεται η προσωπικότητα ή/και η συμπεριφορά κάποιου ατόμου, έστω ως προς κάποιον μόνο τομέα (π.χ. να προβλέπονται τα ενδιαφέροντά του, οι συνήθειές του, οι οικονομικές του δραστηριότητες κτλ.)

Στο Διαδίκτυο, οι επισκέψεις μας σε διάφορες ιστοσελίδες μπορούν κάλλιστα να οδηγήσουν σε δημιουργία προφίλ μας (π.χ. κάποιος μπορεί να αναγνωρίσει, παρατηρώντας το «σερφάρισμά» μας στο Διαδίκτυο, τι μουσική ακούμε ή ποια μέρη αναζητούμε για διακοπές). Ο ανωτέρω κίνδυνος ελλοχεύει σε μεγάλο βαθμό, λόγω των λεγόμενων cookies[1]. Με τον όρο cookies αναφερόμαστε σε μικρά αρχεία με πληροφορίες που μια ιστοσελίδα (συγκεκριμένα ο εξυπηρετητής του ιστού web-server ) αποθηκεύει στον υπολογιστή ενός χρήστη, ώστε κάθε φορά που ο χρήστης συνδέεται στην ιστοσελίδα, η ιστοσελίδα ανακτά τις εν λόγω πληροφορίες και προσφέρει στο χρήστη σχετικές με αυτές υπηρεσίες.

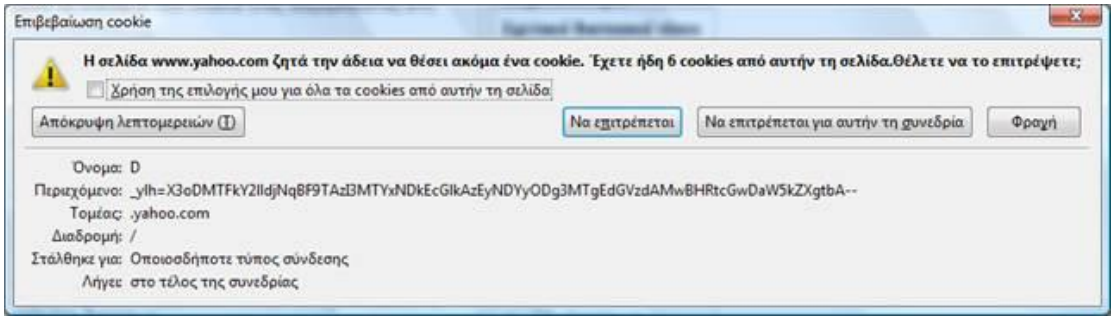
Ειδικότερα, τα cookies είναι μικρά αρχεία κειμένου (.txt) μεγέθους 1Kb περίπου τα οποία δημιουργούνται στον υπολογιστή μας κατόπιν αιτήσεως μιας ιστοσελίδας που επισκεφτόμαστε . Για παράδειγμα, σε λειτουργικό σύστημα Windows XP, τα cookies είναι αποθηκευμένα σε ομώνυμο φάκελο – συγκεκριμένα, στον κατάλογο:

**C:\Documents and Settings\ [όνομα χρήστη]\Local Settings\Cookies.**

Αποτέλεσμα των cookies είναι η δημιουργία ενός πιο «προσωπικού» ανά χρήστη περιεχομένου το οποίο ταιριάζει απόλυτα σε κάθε επιθυμία και ανάγκη του χρήστη, έτσι όταν ο χρήστης πηγαίνει στο συγκεκριμένο site το σύστημα «θυμάται» ,και προσαρμόζει αναλόγως το περιεχόμενο του, βάση των επιλογών του χρήστη . Επιπλέον και οι διαφημίσεις του site προσαρμόζονται βάση των προηγούμενων αναζητήσεων από τις επιλογές του υποκειμένου στα προϊόντα που έχουν καταγραφεί όλα αυτά είναι εγγεγραμμένα στα cookies.

[1] Δεν υπάρχει δόκιμος όρος στα ελληνικά, οπότε προτιμάται η χρήση του αγγλικού όρου που είναι ευρέως γνωστός και καθιερωμένος, προκειμένου να μη δημιουργείται σύγχυση στον αναγνώστη

Στην ήδη ισχύουσα νομοθεσία και συγκεκριμένα στο άρθρο 11 του Ν.2472/1997, αναφέρεται ότι η εγκατάσταση των «cookies» επιτρέπεται μόνο με τη συγκατάθεση του χρήστη και μετά από κατάλληλη ενημέρωσή του.

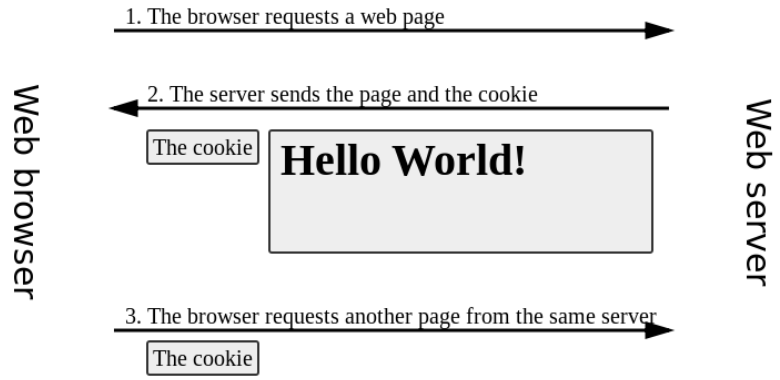



**Εικόνα 1 , όπου ένα site ζητά την άδεια για χρήση cookie.**

### 3.1.1 Χαρακτηριστικά των COOKIES

Τα cookies χρησιμεύουν στους διακομιστές Web ως μια μέθοδος διατήρησης πληροφοριών κατάστασης σχετικά με τον τρόπο με τον οποίο περιηγούνται οι χρήστες στην τοποθεσία. Από αυτά τα υπάρχουν τα cookies **πρώτου μέρους** (first-party cookies) τα οποία εγκαθίσταται από τον υπεύθυνο επεξεργασίας , ο οποίος χειρίζεται τον δικτυακό τόπο που επισκέπτεται ο χρήστης,.

**Εικόνα 2 , όπου φαίνεται η λειτουργία του cookie**



Υπάρχουν δύο ειδών cookies:

- το μόνιμο cookie «έμμονο» (persistent cookie)
- και το cookie περιόδου λειτουργίας «προσωρινό» ( session cookie)

Τα μόνιμα cookies αποθηκεύονται για ένα χρονικό διάστημα το οποίο ορίζει ο διακομιστής Web όταν τοποθετεί το cookie στο πρόγραμμα περιήγησης. Αυτά τα cookies χρησιμοποιούνται για την αποθήκευση πληροφοριών κατάστασης ανάμεσα στις επισκέψεις σε μια τοποθεσία.

Τα cookies συνόδου χρησιμοποιούνται για την αποθήκευση πληροφοριών κατάστασης μόνο εντός μιας συνόδου (για παράδειγμα, για όσο χρονικό διάστημα ο χρήστης έχει συνδεθεί με διαπιστευτήρια – "Log in").. Αυτά τα cookies αποθηκεύονται στη μνήμη cache μόνο κατά τη διάρκεια της επίσκεψης του χρήστη στο διακομιστή, εκδίδοντας το cookie συνόδου και διαγράφονται από τη μνήμη cache όταν ο χρήστης τερματίσει την περίοδο λειτουργίας.

Η εγκατάσταση cookies στον υπολογιστή μας και η περαιτέρω ανταλλαγή τους αποτελεί επεξεργασία προσωπικών δεδομένων. Ως εκ τούτου, πρέπει να πληρούνται σωρευτικά όλες οι προϋποθέσεις που περιγράφονται στο Κεφάλαιο 2. Συνεπώς, προκύπτει από το υπάρχον θεσμικό πλαίσιο ότι για την εγκατάστασή τους στον υπολογιστή ενός χρήστη απαιτείται η προηγούμενη συγκατάθεσή του, καθώς βέβαια και η προηγούμενη σχετική ενημέρωσή του. Ωστόσο, υπάρχουν περιπτώσεις όπου ένα τέτοιο κριτήριο είναι εξαιρετικά αυστηρό: με άλλα λόγια υπάρχουν περιπτώσεις cookies που μπορεί να θεωρηθεί ότι εμπίπτουν στην εξαίρεση όπου μπορεί να γίνει η επεξεργασία και χωρίς προηγούμενη συγκατάθεση, Σύμφωνα με τη σχετική Οδηγία της Ομάδας Εργασίας του Άρθρου 29 για την περίπτωση των cookies [4]. επιτρέπεται η χρήση των cookies χωρίς την υποχρέωση λήψης συγκατάθεσης μόνο και εφόσον εκπληρώνουν ένα από τα δύο κριτήρια :

- **ΚΡΙΤΗΡΙΟ Α:** το cookie χρησιμοποιείται «με αποκλειστικό σκοπό τη διενέργεια της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών».
- **ΚΡΙΤΗΡΙΟ Β:** το cookie «είναι απολύτως αναγκαίο για να μπορεί ο πάροχος υπηρεσίας της κοινωνίας της πληροφορίας την οποία έχει ζητήσει ρητά ο συνδρομητής ή ο χρήστης να παρέχει τη συγκεκριμένη υπηρεσία».

Αναφορικά με το κριτήριο Α, υπάρχουν τρία στοιχεία τουλάχιστον τα οποία είναι δυνατόν να θεωρηθούν ως απολύτως αναγκαία για την μέσω δικτύου επικοινωνία μεταξύ δύο μερών :

1) Η ικανότητα δρομολόγησης της πληροφορίας μέσω του δικτύου, μεταξύ άλλων, με τον προσδιορισμό των σημείων απόληξης της επικοινωνίας.
2) Η ικανότητα ανταλλαγής στοιχείων δεδομένων με τη σκοπούμενη σειρά, μεταξύ άλλων, με την αρίθμηση δεσμίδων δεδομένων.
3) Η ικανότητα ανίχνευσης σφαλμάτων κατά τη διαβίβαση.

Έτσι εάν κάποιο cookie χρησιμοποιείται για κάποιον από τους ανωτέρω σκοπούς, τότε εμπίπτει στο κριτήριο Α.
Αντίστοιχα, για το κριτήριο Β – το οποίο διασφαλίζει την αυστηρότητα της απαλλαγής υποχρέωσης λήψης συγκατάθεσης, θα πρέπει το cookie να εκπληρώνει συγχρόνως τις ακόλουθες δύο προϋποθέσεις:

1) Η χρήση ενός cookie είναι αναγκαία για την παροχή μιας συγκεκριμένης λειτουργικής δυνατότητας/υπηρεσίας στον χρήστη (ή τον συνδρομητή)· αυτό σημαίνει ότι σε περίπτωση απενεργοποίησης των cookies, η λειτουργική δυνατότητα δεν είναι διαθέσιμη.
2) Η συγκεκριμένη λειτουργική δυνατότητα έχει ζητηθεί ρητώς από τον χρήστη (ή τον συνδρομητή), ως στοιχείο μιας υπηρεσίας της κοινωνίας της πληροφορίας.

Συνοψίζοντας τα δύο κριτήρια κατανοούμε ότι για να μπορέσει να εφαρμοστεί η απαλλαγή υποχρέωσης λήψης συγκατάθεσης του χρήστη, πρέπει να υφίσταται ευκρινής συνάφεια μεταξύ της απόλυτης αναγκαιότητας ενός cookie και της παροχής της υπηρεσίας που έχει ζητηθεί ρητώς από τον χρήστη.

Εκτός από τα cookies πρώτου μέρους, υπάρχουν και τα λεγόμενα **«cookie τρίτου μέρους» (third-party cookies).** Τα cookie τρίτου μέρους προέρχονται από άλλες πηγές, οι οποίες διαθέτουν στοιχεία, όπως διαφημίσεις ή εικόνες, ενσωματωμένες στη σελίδα που επισκέπτεται ο χρήστης. Επομένως, με τον όρο **«cookie τρίτου μέρους»** νοείται κανονικά ένα cookie το οποίο έχει εγκατασταθεί από έναν υπεύθυνο της επεξεργασίας ο οποίος δεν συμπίπτει με τον υπεύθυνο της επεξεργασίας ο οποίος χειρίζεται τον δικτυακό τόπο που επισκέπτεται ο χρήστης (όπως αυτός προσδιορίζεται με βάση τον τρέχοντα URL που εμφανίζεται στη γραμμή

διευθύνσεων του φυλλομετρητή) έτσι η έννοια του τρίτου cookie ορίζεται αποκλειστικά με γνώμονα τη δομή URL που εμφανίζεται στην γραμμή διευθύνσεων του φυλλομετρητή, και εγκαθίσταται από δικτυακούς τόπους ανήκοντες σε περιοχή διαφορετική από την περιοχή του δικτυακού τόπου τον οποίο επισκέπτεται ο χρήστης , που όμως εμφανίζεται στην γραμμή διευθύνσεων του φυλλομετρητή χωρίς να έχει σημασία το κατά πόσο η εν λόγω οντότητα είναι διακριτός υπεύθυνος επεξεργασίας ή όχι.

### 3.1.2 Περιγραφή των cookies

Στα Cookies αποθηκεύονται πληροφορίες προσωπικές για τον κάθε χρήστη, όπως πότε έγινε η τελευταία επίσκεψή του χρήστη. Δεν μπορούν από μόνα τους να «μάθουν» ούτε το όνομα του χρήστη ούτε κάτι άλλο και, βέβαια, από μόνα τους δεν μπορούν να το μεταβιβάσουν πουθενά. Έτσι δεν αποτελούν απειλή για την ασφάλεια του προσώπου, αποτελούν όμως (υπό προϋποθέσεις) εισβολή στην προσωπική ζωή, καθώς ουσιαστικά δεν περιέχουν προσωπικές πληροφορίες αλλά έναν αριθμό αναγνώρισης.

Έτσι, για παράδειγμα, όταν ένας χρήστης επισκέπτεται sites που περιέχουν cookies από μια συγκεκριμένη διαφημιστική εταιρεία, ο server της εταιρείας αυτής μπορεί να διαβάσει τον αριθμό αναγνώρισης και να κάνει τις συσχετίσεις του. Αν, όμως, ο χρήστης συμπληρώσει κάποια διαδικτυακή (online) φόρμα και στείλει στοιχεία, τότε ο αριθμός αυτός μπορεί να συνδεθεί και με το όνομά του ή με περισσότερα προσωπικά στοιχεία. Θεωρούμε βέβαιο ότι στη συντριπτική πλειονότητα -αν όχι ολότητα - των χρηστών δεν αρέσει να παρακολουθούνται, πόσο μάλλον όταν δεν το ξέρουν καν.

Τέλος τα cookies δεν μπορούν να αποθηκεύσουν περισσότερα στοιχεία από όσα ο χρήστης τους επιτρέπει συμπληρώνοντας κάποια φόρμα. Επιπλέον είναι γνωστό ότι τα cookies δεν αποτελούν απειλή για τον υπολογιστή του χρήστη. Καθώς ένα cookie δεν είναι εκτελέσιμο αρχείο (είναι απλώς ένα αρχείο κειμένου) και δεν είναι σε θέση να εκτελέσει εντολές που θα μπορούσαν, για παράδειγμα, να διαγράψουν τα περιεχόμενα ενός σκληρού δίσκου.
Ένα cookie δεν αποτελείται απλώς από ένα όνομα και μία τιμή. Υπάρχουν συνολικά έξι παράμετροι που μπορούν να περιλαμβάνονται σε ένα cookie, αλλά από αυτές τις έξι μόνο δύο είναι υποχρεωτικές.

Συγκεκριμένα, οι παράμετροι είναι:

1) Το όνομα (υποχρεωτικό), η τιμή του (υποχρεωτική), η ημερομηνία λήξης του, το "μονοπάτι" (path), το «πεδίο» (domain) και το αν απαιτείται ασφαλής διακομιστής (secure server) για να λειτουργήσει το cookie.
2) Η τιμή και το όνομα του cookie είναι συνδεδεμένα μεταξύ τους, αφού ορίζονται ως name=value. Η τιμή μπορεί να είναι NULL, ώστε να μηδενίσει την όποια τιμή ήδη υπάρχει σε ένα cookies.
3) Η ημερομηνία ορίζει τη διάρκεια ζωής ενός cookie και, σε περίπτωση που δε δοθεί, ορίζεται αυτόματα στη διάρκεια μιας συνόδου (session) Ένα session μπορεί να διαφέρει ανάλογα με την πλατφόρμα και το πρόγραμμα πλοήγησης (browser), αλλά γενικά διαρκεί για όσο διάστημα ο browser είναι ανοικτός.
4) Η παράμετρος «path» ορίζει ποιες σελίδες θα μπορούν να διαβάσουν το cookie και ποιες όχι. Αν δεν οριστεί τιμή, τότε το cookie παίρνει το path της σελίδας που το δημιούργησε.
5) Το domain, στην ουσία, είναι μία παράμετρος που επεκτείνει το path, αφού ορίζει το domain στο οποίο είναι ενεργό το cookie. Αυτό είναι πολύ χρήσιμο σε domains των οποίων το περιεχόμενο βρίσκεται σε περισσότερους από έναν servers. Σε περίπτωση που δεν οριστεί τιμή, παίρνει ως τιμή το domain στο οποίο βρίσκεται η σελίδα που το δημιούργησε.
6) Η παράμετρος secure ορίζει αν το cookie θα λειτουργεί μόνο κάτω από Secure serves, ενώ η προκαθορισμένη τιμή είναι "False", αφού τα περισσότερα sites δε βρίσκονται σε Secure server.

### 3.1.3 Αξιολόγηση αναγκαιότητας των COOKIES

Τα cookies τα οποία μπορούν και απαλλάσσονται από την υποχρέωση λήψης συγκατάθεσης κατόπιν ενημέρωσης υπό ορισμένες προϋποθέσεις και εφόσον δεν χρησιμοποιούνται για πρόσθετους σκοπούς είναι :

1) τα cookies εισαγωγής δεδομένων χρήστη (αναγνώριση ταυτότητας συνόδου), για την διάρκεια της συνόδου ή τα μόνιμα cookies με διάρκεια ζωής μονο λίγων ωρών, σε ορισμένες περιπτώσεις.
2) Τα cookies επαλήθευσης ταυτότητας, εφόσον χρησιμοποιούνται για υπηρεσίες που προϋποθέτουν επαλήθευση της ταυτότητας για την διάρκεια της συνόδου.

3) Τα χρηστοκεντρικά cookies ασφαλείας , τα οποία χρησιμοποιούνται για την ανίχνευση καταχρήσεων στον τομέα της επαλήθευσης της ταυτότητας, για περιορισμένο και συνεχές χρονικό διάστημα .
4) Τα cookies συνόδου που χρησιμοποιούνται ανάγνωση περιεχομένου πολυμέσων, πχ. Cookies του τύπου «flash player»για την διάρκεια της συνόδου.
5) Cookies εξισορρόπησης φορτίου συνόδου, για τη διάρκεια της συνόδου
6) Μόνιμα cookies για την εξατομίκευσης διεπαφής χρήστη, για την διάρκεια της συνόδου (ή για ελαφρώς μεγαλύτερο χρονικό διάστημα)
7) Cookies τρίτου μέρους που χρησιμεύουν για τη ανταλλαγή δεδομένων κοινωνικών δικτύων (μέσω συνδεόμενης υπομονάδας), για τα μέλη ενός κοινωνικού δικτύου που έχουν συνδεθεί μέσω προσωπικού κωδικού.

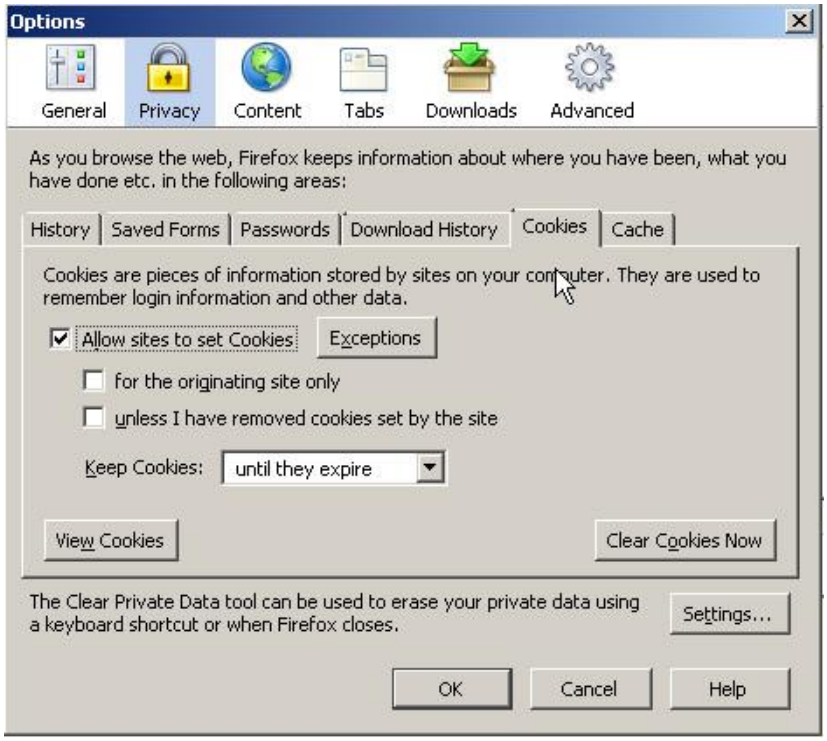
Για την τελευταία περίπτωση (χρήση cookies τρίτου μέρους που χρησιμεύουν για την ανταλλαγή δεδομένων κοινωνικής δικτύωσης) για σκοπούς άλλους από την παροχή μια λειτουργικής δυνατότητας που έχει ζητηθεί ρητά από τα μέλη του εκάστοτε δικτύου προϋποθέτει τη λήψη συγκατάθεσης, ιδίως αν οι σκοποί αυτοι περιλαμβάνουν την ιχνηλάτηση του χρήστη σε διάφορους δικτυακούς τόπους.

### 3.1.4 Διαγραφή των COOKIES

Ο χρήστης μπορεί να πραγματοποιήσει την διαγραφή των cookies με εύκολο σχετικά τρόπο από τον υπολογιστή του. Η διαγραφή των αρχείων αυτών μπορεί να γίνει και από τον Internet Explorer μέσα από το παράθυρο επιλογών που εμφανίζεται επιλέγοντας «Tools - Internet Options» «<Εργαλεία - Επιλογές Internet...»). Από την καρτέλα «General » «Γενικά») διαγράφουμε τα αρχεία cookies πατώντας το κουμπί «Delete Cookies...» «Διαγραφή Cookies...»)

Με την παραπάνω ενέργεια θα διαγραφούν όλα αδιακρίτως τα Cookies είτε είναι βοηθητικά πλοήγησης είτε «ιχνηλατικά». Εάν κανείς θέλει να διαγράψει μόνο τα «ιχνηλατικά» τότε υπάρχουν ειδικά προγράμματα καταπολέμησης προγραμμάτων κατασκοπευτικού περιεχομένου. – τα λεγόμενα προγράμματα "anti- Spyware".

Ειδικότερα, με τον όρο spyware ορίζονται προγράμματα που παρακολουθούν και συλλέγουν πληροφορίες για την δραστηριότητα ενός συστήματος χωρίς την έγκριση του διαχειριστή ή του χρήστη. Οι πληροφορίες που συλλέγονται ποικίλουν από στοιχεία επισκεψιμότητας σε σελίδες (tracking) μέχρι και πλήρη καταγραφή ευαίσθητων πληροφοριών όπως πληκτρολόγηση κωδικών, κλπ.




**Εικόνα 3**

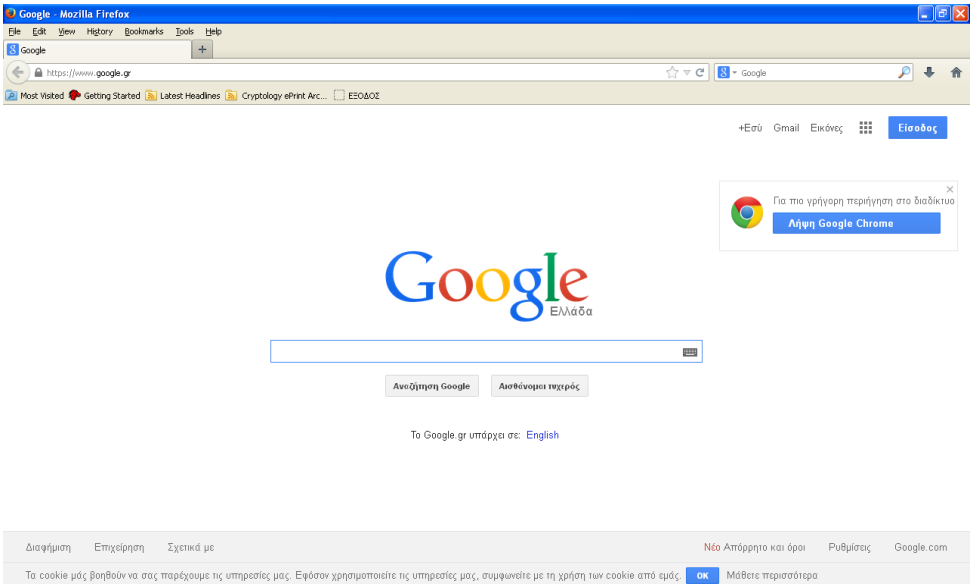
**Όπου επιτρέπεται η αποδοχή cookies από τον χρήστη του ιντερντετ.**

### 3.1.5 Συγκατάθεση για τη λήψη cookies

Νωρίτερα είδαμε τις περιπτώσεις εκείνες όπου επιτρέπεται η εγκατάσταση cookie και χωρίς τη συγκατάθεση του χρήστη (π.χ. cookie συνόδου, το οποίο είναι απαραίτητο για να ταυτοποιείται ο χρήστης άπαξ και έχει συνδεθεί σε μία διαδικτυακή υπηρεσία με συνθηματικό), καθώς και τις περιπτώσεις όπου απαιτείται η συγκατάθεση (π.χ. cookies για μέτρηση στοιχείων επισκεψιμότητας του site, τα οποία δεν είναι απολύτως απαραίτητα για την παροχή της προσφερόμενης διαδικτυακής υπηρεσίας). Στο σημείο αυτό, πρέπει να ανακαλέσουμε τα όσα προβλέπει το υπάρχον νομικό πλαίσιο για τη συγκατάθεση (Κεφ. 2). Η συγκατάθεση πρέπει να είναι σαφής, ρητή και ειδική. Ως εκ τούτου, αν απλά το πρόγραμμα πλοήγησης είναι ρυθμισμένο κατάλληλα ώστε να αποδέχεται όλων των ειδών τα cookies, αυτό δεν μπορεί να εκληφθεί ως

συγκατάθεση του χρήστη (διότι, απλά, ο τελευταίος μπορεί να μην γνωρίζει τις ανωτέρω ρυθμίσεις).

Πλέον, η πλειοψηφία των μεγάλων παρόχων διαδικτυακών υπηρεσιών έχουν λάβει μέριμνα για λήψη ρητής συγκατάθεσης του χρήστη (βλ., για παράδειγμα, κάτω τμήμα της Εικόνας 4 – ωστόσο, το πρόβλημα δεν έχει ακόμα πλήρως επιλυθεί.




**Εικόνα 4 – Αρχική σελίδα της Google,**
**όπου ζητείται συγκατάθεση του χρήστη για λήψη cookies**

## 3.2 Κοινωνικά δίκτυα (social networks)

Μία γνωστή ρήση, που ενδεχομένως έχουμε ακούσει από τους γονείς μας, είναι «μοναχός σου ούτε στον παράδεισο» και είναι φράση πολύ γνωστή από όλους και δηλώνει την ανάγκη του ανθρώπου για επικοινωνία. Η αλματώδης ανάπτυξη της τεχνολογίας στις μέρες μας διεύρυνε τα χωρικά όρια όλων των κοινωνικών ομάδων και των τοπικών κοινωνικών δικτύων , δημιουργώντας έτσι ένα μωσαϊκό από δίκτυα και υπό – δίκτυα που απλώνονται σε όλο τον κόσμο – τα κοινωνικά δίκτυα.

**Εικόνα 3.3 – Διασύνδεση ατόμων σε ένα κοινωνικό δίκτυο**

Ο όρος μέσα κοινωνικής δικτύωσης (ή αλλιώς social media) αναφέρεται στα μέσα αλληλεπίδρασης ομάδων ανθρώπων μέσω διαδικτυακών κοινοτήτων. Τα social media εμφανίζονται σε διάφορες μορφές όπως πχ. ιστολόγια, ιστοσελίδες όπως το Facebook, φόρουμς, κλπ. (Wikipedia.2013)

Όλα τα κοινωνικά δίκτυα έχουν τα εξής κοινά χαρακτηριστικά :

1. Ο χρήστης δημιουργεί ένα προσωπικό προφίλ βασισμένο στα προσωπικά του δεδομένα
2. Παρέχεται η δυνατότητα στους χρήστες να δημοσιεύσουν προσωπικές τους φωτογραφίες ή βίντεο στο προφίλ τους ή άλλες προσωπικές καταχωρήσεις (σκέψεις, μουσική από άλλους δικτυακούς τόπους, κλπ)
3. Κάθε χρήστης έχει έναν κατάλογο «επαφών» από ο οποίος εμπλουτίζεται από άλλους χρήστες με τους οποίους μπορούν να έρθουν σε διαδικτυακή συνομιλία.

### 3.2.1 Πρόσβαση «τρίτων»

Οι υπηρεσίες κοινωνικής δικτύωσης παρέχονται δωρεάν στου χρήστες τους ,τα έσοδά τους προέρχονται κυρίως από τις διαφημίσεις οι οποίες παρέχεται από τρίτους πάροχους οι οποίες εμφανίζονται σε συγκεκριμένα μέρη των ιστοσελίδων παράλληλα με τις ιστοσελίδες που δημιουργούν και χρησιμοποιούν οι χρήστες.

Οι πάροχοι των διαφημίσεων συνήθως χρησιμοποιούν την λειτουργία «στοχευόμενων διαφημίσεων» (οι οποίες πραγματοποιούνται με τη χρήση cookies) όπου μέσω «παρακολούθησης» των προσωπικών μας προτιμήσεων , πληροφοριών,
και των διάφορων ιστότοπων των οποίων επισκεπτόμαστε καθώς και τα προϊόντα τα οποία αναζητούμε στο διαδίκτυο μας εμφανίζουν στο χώρο των διαφημίσεων και την ανάλογη διαφήμιση βάση των δικών μας προτιμήσεων .

Επιπλέον οι υπηρεσίες κοινωνικής δικτύωσης προτείνουν στους χρήστες τους και πολλές επιπρόσθετες εφαρμογές οι οποίες παρέχονται από τρίτους πάροχους, όπου όμως και πάλι επεξεργάζονται τρίτοι τα δεδομένα προσωπικού χαρακτήρα των χρηστών , φυσικά απαραίτητη προϋπόθεση για να χρησιμοποιήσει την εφαρμογή αυτή ο χρήστης είναι η αποδοχή των όρων της εφαρμογής και η ταυτόχρονη υπογραφή του χρήστη ότι επιτρέπει να γίνει επεξεργασία όλων των προσωπικών δεδομένων που βρίσκονται στο προφίλ του. Τέτοιου είδους εφαρμογές είναι μπορεί να είναι παιχνίδια, ή διάφορες ενημερωτικές εφαρμογές.

Έτσι εδώ θα πρέπει να τονιστεί ότι ο πάροχος των υπηρεσιών κοινωνικής δικτύωσης θα πρέπει να διαθέτει όλα τα απαιτούμενα μέσα για να διασφαλίσει ότι οι εφαρμογές «τρίτων» που χρησιμοποιούν οι χρήστες είναι απολύτως σύμφωνες με το νομικό πλαίσιο προστασίας προσωπικών δεδομένων , και για να γίνει αυτό απαιτείται να υπάρχουν σαφείς και συγκεκριμένες πληροφορίες στους χρήστες σχετικά με το είδος της επεξεργασίας των προσωπικών τους πληροφοριών που πρόκειται να γίνει , μέσω της κάθε εφαρμογής .

Φυσικά αυτό είναι ένα από τα πολύ αμφιλεγόμενα θέματα τα οποία εξετάζονται στον νέο κανονισμό καθώς αμφισβητείται σε έντονο βαθμό κατά πόσο είναι ασφαλή τα προσωπικά μας δεδομένα, και κατά πόσο ο «τρίτος» έχει δικαίωμα πρόσβασης στις προσωπικές μας πληροφορίες .

Επομένως, οι υπηρεσίες κοινωνικής δικτύωσης θα πρέπει να λειτουργούν με απόλυτο σεβασμό στον άνθρωπο και κατ' επέκταση στα δικαιώματα και τις ελευθερίες των χρηστών, οι οποίοι δικαιούνται να απαιτούν ότι όλα τα δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν υφίστανται επεξεργασία η οποία είναι απολύτως σύμφωνη με την εθνική νομοθεσία και την ευρωπαϊκή νομοθεσία περί ιδιωτικής ζωής και προστασίας των προσωπικών δεδομένων.

### 3.2.2 Υπεύθυνος επεξεργασίας δεδομένων στα κοινωνικά δίκτυα

Στα κοινωνικά δίκτυα οι υπεύθυνοι επεξεργασίας των προσωπικών δεδομένων είναι ο πάροχος των υπηρεσιών της κοινωνικής δικτύωσης , και είναι αυτός που καθορίζει τη χρήση των δεδομένων του χρήστη και είναι επιπλέον υπεύθυνος για την εμπορική προώθηση των διαφημίσεων που παρέχεται στα κοινωνικά δίκτυα από ξένους πάροχους.

(Υπενθυμίζεται ότι όπως αναφέρθηκε στο κεφάλαιο 2 <υπεύθυνος της επεξεργασίας>, είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος φορέας που μόνος ή από κοινού με άλλους καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα [άρθρο της οδηγίας 95/46] )

Οι υπεύθυνοι επεξεργασίας των κοινωνικών δικτύων έχουν πολύ μεγάλες ευθύνες καθώς θα πρέπει να φανούν άξιοι στην εμπιστοσύνη χιλιάδων χρηστών που δημιουργούν προσωπικά προφίλ με τα προσωπικά τους δεδομένα, και να λάβουν όλα τα απαραίτητα μέτρα προκειμένου να διασφαλιστεί η μέγιστη ασφάλεια προσωπικών δεδομένων των χρηστών.
Έτσι θα πρέπει να δοθεί μεγάλη προσοχή κατά την φάση στου σχεδιασμού ενός κοινωνικού δικτύου και να δημιουργηθούν οι κατάλληλες ρυθμίσεις στην δημιουργία των προφίλ ώστε να υπάρχουν οι κατάλληλοι περιορισμοί στην πρόσβαση των προφίλ των χρηστών για να μην έχουν πρόσβαση «τρίτοι» στις προσωπικές πληροφορίες των χρηστών , είτε όσον αφορά τρίτους παρόχους είτε όσον αφορά τις διάφορες μηχανές αναζήτησης του διαδικτύου.

### 3.2.3 Πάροχοι εφαρμογών

Όλοι οι πάροχοι εφαρμογών είναι και υπεύθυνοι επεξεργασίας δεδομένων, εφόσον αναπτύσσουν εφαρμογές που λειτουργούν επιπλέον εκείνων του παρόχου των υπηρεσιών κοινωνικής δικτύωσης και τις οποίες ο χρήστης αποφασίζει εάν θα χρησιμοποιήσει.
Επομένως, είναι σημαντικό οι υπηρεσίες κοινωνικής δικτύωσης να λειτουργούν κατά τρόπο τέτοιο που να σέβονται τα δικαιώματα και τις ελευθερίες των χρηστών, οι οποίοι δικαιούνται να προσδοκούν ότι τα δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν υφίστανται επεξεργασία σύμφωνα με την ευρωπαϊκή και την εθνική νομοθεσία περί ιδιωτικής ζωής και προστασίας των δεδομένων.

Όλοι οι πάροχοι υπηρεσιών κοινωνικής δικτύωσης είναι υποχρεωμένοι :

- Να ενημερώνουν τους χρήστες τους σχετικά με την εφαρμογή που πρόκειται να χρησιμοποιήσουν ,
- Τους σκοπούς και το είδος της επεξεργασίας των προσωπικών δεδομένων .
- Επιπλέον θα πρέπει, να υπάρχει σαφή ενημέρωση σχετικά με τους κινδύνους της ιδιωτικής ζωής , όταν αναρτούν πληροφορίες αυτοβούλως οι χρήστες ,
- Και να δίνετε ιδιαίτερη προσοχή όταν το ανέβασμα πληροφοριών για άλλα άτομα είναι παράβαση της ιδιωτικής ζωής των προσωπικών δεδομένων .

Οι υπηρεσίες κοινωνικής δικτύωσης διευκολύνουν τους «τρίτους» παρόχους καθώς δημοσιεύουν τον τρόπο με τον οποίο μπορεί ένας «τρίτος» πάροχος να δημιουργήσει ένα λογισμικό υπό τη μορφή «διασύνδεση προγραμματισμού εφαρμογών» (Application Programming Interface – API ).
Και έτσι δημιουργούνται οι διάφορες εφαρμογές από τρίτους παρόχους που συναντάμε στα κοινωνικά δίκτυα.

Κατά την παροχή μιας API η οποία δίνει πρόσβαση σε δεδομένα επαφών , ο πάροχος της υπηρεσίας της κοινωνικής δικτύωσης θα πρέπει :

- Να ορίζει το επίπεδο πρόσβασης του «τρίτου παρόχου» , στο προφιλ του χρήστη θα πρέπει να έχει μόνο την δυνατότητα εκτέλεσης μιας συγκεκριμένης εργασίας (εφαρμογής)

Έτσι ο τρίτος πάροχος θα μπορεί να έχει περιορισμένη πρόσβαση στα δεδομένα προσωπικού χαρακτήρα των χρηστών και μόνο για το χρονικό διάστημα που θα εκτελείται η συγκεκριμένη εφαρμογή (πχ. Παιχνίδι).

### 3.2.4 Διατήρηση δεδομένων

Η διατήρηση των δεδομένων στα κοινωνικά δίκτυα θα πρέπει να γίνεται με μεγάλη προσοχή και να δίνεται έντονη εμφάνιση στις διαγραφές δηλαδή :

Όλα τα δεδομένα προσωπικού χαρακτήρα που έχει αναρτήσει ένας χρήστης κατά την χρησιμοποίηση μιας υπηρεσίας κοινωνικής δικτύωσης θα πρέπει να διαγράφονται αυτομάτως μόλις ο χρήστης διαγράψει τον λογαριασμό του . Το ίδιο θα πρέπει να συμβεί και στην αντίστροφη περίπτωση όπου ο πάροχος της κοινωνικής υπηρεσίας αποφασίσει να διαγράψει την εφαρμογή από τον χώρο του διαδικτύου, τότε θα πρέπει όλα τα προσωπικά δεδομένα των χρηστών να σβηστούν εντελώς, από οποιαδήποτε μεριά του διαδικτύου .

Επιπλέον οποιαδήποτε πληροφορία αναρτηθεί αρχικά από έναν χρήστη αλλά στην πορεία ο χρήστης αποφασίσει να την διαγράψει τότε η συγκεκριμένη πληροφορία θα πρέπει να διαγραφεί οριστικά και να μην διατηρηθεί πουθενά στο διαδίκτυο.

Τέλος όταν ένας χρήστης δεν χρησιμοποιεί τον λογαριασμό του για αρκετό χρονικό διάστημα τότε θα πρέπει το προφίλ του να μπαίνει σε μορφή αδράνειας δηλαδή να μην είναι εμφανές στους υπόλοιπους χρήστες , επίσης μετά από κάποιο διάστημα όπου ένα προφίλ είναι σε αδράνεια τότε θα πρέπει να διαγράφεται οριστικά .

Ωστόσο για περισσότερες πληροφορίες σχετικά με την προστασία της ιδιωτικότητας του ένας χρήστης μπορεί να επισκεφτεί την ιστοσελίδα της Ευρωπαϊκής Ένωσης Διαδραστικών και Ψηφιακών Διαφημίσεων (E.D.A.A.) [**http://www.youronlinechoices.com/gr/**]

Ένας από τους πιο γνωστούς πλέον ιστοχώρους κοινωνικής δικτύωσης είναι το Facebook , που έκανε την εμφάνιση του στις αρχές του 2004 και από τότε κυριολεκτικά κατακτήσει τον κόσμο του διαδικτύου.

## 3.3 Αναγνώριση Προσώπων (Facial recognition)

Η τεχνολογική αναγνώριση προσώπων δεν είναι κάτι το νέο , όμως με την συνεχώς αυξανόμενη χρήση της συγκεκριμένης τεχνολογίας εγείρονται σοβαρές ανησυχίες ως προς την παραβίαση του απορρήτου, και των ατομικών ελευθεριών .

Κάτι τέτοιο είναι εμφανές με τις πρόσφατες εξελίξεις της τεχνολογίας και την εφαρμογή της αναγνώρισης προσώπου τόσο στις ψηφιακές εικόνες δύο διαστάσεων, που είναι μια φωτογραφία σε ψηφιακή μορφή, όσο και στις τρισδιάστατες εικόνες ή αλλιώς κινούμενες εικόνες που αφορούν τα βίντεο. Η αναγνώριση προσώπων των προσώπων γίνεται με την αυτόματη επεξεργασία των ψηφιακών εικόνων οι οποίες περιέχουν πρόσωπα ατόμων , με σκοπό την ταυτοποίηση , εξακρίβωση / επαλήθευση ή κατηγοριοποίηση των συγκεκριμένων ατόμων .

Η αρχική χρήση της μεθόδου χρησιμοποιούταν σε συστήματα ασφαλείας και μαζί με άλλες βιομετρικές μεθόδους όπως η αναγνώριση δαχτυλικών αποτυπωμάτων ή αναγνώριση αμφιβληστροειδούς χιτώνα για την αναγνώριση υπόπτων.

Ωστόσο τα τελευταία έτη, εμφανίζεται σε πολλές διαδικτυακές εφαρμογές, πρόσφατα έκανε την εμφάνιση της στο facebook με την εφαρμογή : «Tag Suggestions», και έδινε την δυνατότητα των χρηστών να χρησιμοποιούν ένα λογισμικό αναγνώρισης προσώπων για να ταυτοποιούν αυτομάτως τους φίλους τους στις φωτογραφίες που δημοσίευαν στο προφίλ τους.

Η λειτουργία της αναγνώριση των προσώπων γίνεται με αλγόριθμους , οι οποίοι αρχικά ανιχνεύουν τα χαρακτηριστικά των πρόσωπων της φωτογραφίας και στην συνέχεια, τα συγκρίνουν με τα πρόσωπα που είναι ήδη καταχωρημένα στην εφαρμογή της Αναγνώριση Προσώπου, τα οποία έχουν καταχωρηθεί μέσω φωτογραφιών ή άλλων δεδομένων . Όσο περισσότερες φωτογραφίες προστίθενται στο σύστημα, τόσο πιο δυνατή γίνεται η εφαρμογή .

Φυσικά υπάρχει το ενδεχόμενο να μην γίνει σωστή η αναγνώριση του προσώπου, ή ακόμα οι αλγόριθμοι που χρησιμοποιούνται από την εφαρμογή για την αναγνώριση προσώπων είναι πιθανό να βρουν συγγενείς των ατόμων της φωτογραφίας σας, λόγω των βασισμένων στη γενετική ομοιοτήτων προσώπου που υπάρχουν ανάμεσα στους συγγενείς.

Σε περίπτωση «λάθους» θα πρέπει «χειροκίνητα» να γίνει ταυτοποίηση των προσώπων , προσθέτοντας όμως συνεχώς νέες φωτογραφίες τότε η εφαρμογή «μαθαίνει» πρόσωπα και είναι σε θέση να τα αναγνωρίσει σωστά σε μελλοντικές φωτογραφίες, ακόμα και σε διαφορετικές ηλικίες της ζωής του ατόμου !!!

Με την υπάρχουσα νομοθεσία (95/46/ΕΚ) και την Γνωμοδότηση 02/2012 όσον αφορά την αναγνώριση προσώπου στις επιγραμμικές και κινητές υπηρεσίες , γίνεται σαφή και κατανοητό ότι οι ψηφιακές εικόνες θεωρούνται δεδομένα προσωπικού χαρακτήρα, όταν τα χαρακτηριστικά των ατόμων είναι ευδιάκριτα και επιτυγχάνεται η ταυτοποίησή του , η μοναδική εξαίρεση έπεται στην περίπτωση μιας εικόνων από μια σκηνές στις οποίες τα άτομα που εμφανίζονται είναι εξ αποστάσεως ή θολά και δεν είναι εφικτή η ταυτοποίηση τους.

Στο άρθρο 6 της οδηγίας 95/46Ε αναφέρονται οι αρχές που πρέπει να τηρούνται ως προς την ποιότητα των δεδομένων.

Τα κράτη μέλη προβλέπουν ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει:

α) να υφίστανται σύννομη και θεμιτή επεξεργασία

β) να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και η μεταγενέστερη επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς. Η μεταγενέστερη επεξεργασία για ιστορικούς, στατιστικούς ή επιστημονικούς σκοπούς δεν θεωρείται ασυμβίβαστη εφόσον τα κράτη μέλη προβλέπουν κατάλληλες εγγυήσεις-

γ) να είναι κατάλληλα, συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται και υφίστανται επεξεργασία-

δ) να είναι ακριβή και, εφόσον χρειάζεται, να ενημερώνονται πρέπει να λαμβάνονται όλα τα εύλογα μέτρα ώστε δεδομένα ανακριβή ή ελλιπή σε σχέση με τους σκοπούς για τους οποίους έχουν συλλέγει ή υφίστανται κατόπιν επεξεργασία, να διαγράφονται ή να διορθώνονται.

ε) να διατηρούνται με μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των προσώπων στα οποία αναφέρονται μόνο κατά τη διάρκεια περιόδου που δεν υπερβαίνει την απαιτούμενη για την επίτευξη των σκοπών για τους οποίους έχουν συλλέγει ή για τους οποίους αργότερα υφίστανται επεξεργασία. Τα κράτη μέλη προβλέπουν κατάλληλες εγγυήσεις για τα δεδομένα προσωπικού χαρακτήρα που διατηρούνται πέραν της περιόδου αυτής για σκοπούς ιστορικούς, στατιστικούς ή επιστημονικούς.

Εναπόκειται στον υπεύθυνο της επεξεργασίας να εξασφαλίσει την τήρηση της παραγράφου 1.

Επιπλέον η επεξεργασία μπορεί να πραγματοποιηθεί μόνο αν τηρούνται ένα από τα κριτήρια που καθορίζονται στο άρθρο 7 της οδηγίας 95/46Ε

### 3.3.1 Βασικές αρχές νόμιμης επεξεργασίας δεδομένων

Τα κράτη μέλη προβλέπουν ότι επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να γίνεται μόνον εάν:

α) το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει τη ρητή συγκατάθεσή του

β) είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το ενδιαφερόμενο πρόσωπο είναι συμβαλλόμενο μέρος ή για την εκτέλεση προσυμβατικών μέτρων ληφθέντων αιτήσει του ή

γ) είναι απαραίτητη για την τήρηση εκ του νόμου υποχρεώσεως του υπευθύνου της επεξεργασίας ή

δ) είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται τα δεδομένα ή

ε) είναι απαραίτητη για την εκπλήρωση έργου δημοσίου συμφέροντος ή εμπίπτοντος στην άσκηση δημοσίας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας ή στον τρίτο στον οποίο ανακοινώνονται τα δεδομένα ή

στ) είναι απαραίτητη για την επίτευξη του εννόμου συμφέροντος που επιδιώκει ο υπεύθυνος της επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα, υπό τον όρο ότι δεν προέχει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του προσώπου στο οποίο αναφέρονται τα δεδομένα που χρήζουν προστασίας δυνάμει του άρθρου 1 παράγραφος 1 της παρούσας οδηγίας.

Έτσι είναι πλέον αυτονόητο ότι λόγω των ιδιαίτερων κινδύνων που συνδέονται με τα βιομετρικά δεδομένα, απαιτείται ο καθορισμός με πλήρη σαφήνεια του σκοπού και τα μέσα της επεξεργασίας καθώς και η εν γνώσει συγκατάθεση του ατόμου πριν την έναρξη της ανάλυσης των ψηφιακών εικόνων για την αναγνώριση προσώπου. Τέλος η χρησιμοποίηση των δεδομένων που έχουν υποστεί επεξεργασία θα πρέπει να γίνεται με αυστηρώς περιορισμένο σκοπό και να διαγράφονται αμέσως στο τέλος της επεξεργασίας, από τον υπεύθυνο επεξεργασίας, Ως υπεύθυνος επεξεργασίας των δεδομένων είναι ο ιδιοκτήτης του διαδικτυακού τόπου και οι πάροχοι των επιγραμμικών υπηρεσιών, καθώς και φορείς που δραστηριοποιούνται στην εφαρμογή της κινητής υπηρεσίας και εμπλέκονται στην αναγνώριση του προσώπου.

Ωστόσο σε ορισμένες περιπτώσεις ο υπεύθυνος της επεξεργασίας των δεδομένων μπορεί προσωρινά να χρειάζεται να εκτελέσει ορισμένα στάδια επεξεργασίας αναγνώρισης προσώπου, για να μπορέσει να καθορίσει κατά πόσον ένας χρήστης έχει δώσει ή όχι την συγκατάθεση του σε αυτή την επεξεργασία .

Αυτή και μόνο η περίπτωση υπόκειται στην δικαιοδοσία του υπευθύνου της επεξεργασίας η ανίχνευση του υποκειμένου καθώς ανήκει στην νομική βάση όπου έχει να κάνει με το έννομο συμφέρον του υπευθύνου της επεξεργασίας των δεδομένων και θα πρέπει τα οποιαδήποτε δεδομένα που χρησιμοποιήθηκαν να αναλυθούν με τρόπο αυστηρά περιορισμένο και με μοναδικό σκοπό τον έλεγχο για της συγκατάθεσης του χρήστη τέλος σε στην περίπτωση μη συγκατάθεσης του υποκειμένου η διαγραφή των δεδομένων θα πρέπει να είναι άμεση.

## 3.4 Υπολογιστικό νέφος (cloud computing)

Ένα από τα τελευταία επιτεύγματα της εξέλιξης της τεχνολογίας είναι το υπολογιστικό νέφος (cloud computing), όπου μία νεφοεφαρμογή που χρησιμοποιεί ειδική αρχιτεκτονική λογισμικού του νέφους και εξαλείφει συχνά την ανάγκη εγκατάστασης και λειτουργίας της εφαρμογής στον υπολογιστή για την χρήση της εφαρμογής αρκεί μόνο η ύπαρξη διαδικτύου.
Με πιο απλά λόγια το cloud computing είναι μία δομή , η οποία μας δίνει την δυνατότητα να έχουμε πρόσβαση και να χρησιμοποιούμε διάφορες διαδικτυακές εφαρμογές με την σύνδεσή μας στον διαδίκτυο, καθώς η όλη δομής της εφαρμογής βρίσκεται σε έναν server στο διαδίκτυο και εμείς μπορούμε να χρησιμοποιούμε την εφαρμογή χωρίς να την έχουμε εγκατεστημένη στον υπολογιστή μας .

Το σύμβολο που έχει καθιερωθεί για το υπολογιστικό νέφος είναι το σύννεφο και με τον τρόπο αυτό περιγράφουμε ένα απομακρυσμένο σύνολο από υπηρεσίες στο οποίο έχουμε πρόσβαση και το χρησιμοποιούμε χωρίς όμως να το έχουμε αποθηκευμένο στον υπολογιστή μας .

Πρόσβαση σε διάφορες νεφοεφαρμογές έχουν οι χρήστες είτε δωρεάν, είτε επί πληρωμή – ανάλογα κάθε φορά με τους όρους τις εφαρμογής που χρησιμοποιούν .

Οι πάροχοι υπηρεσιών υπολογιστικού νέφους προσφέρουν μεγάλο φάσμα υπηρεσιών οποίες μπορεί να είναι:

- συστήματα εικονικής επεξεργασίας,
- υπηρεσίες που προσφέρουν μεγάλο όγκο αποθήκευσης δεδομένων ,

- διάφορες εφαρμογές οι οποίες λειτουργούν απευθείας στο διαδίκτυο όπως ημερολόγιο, email, επεξεργασία κειμένου κ.α

### 3.4.1 Πλεονεκτήματα cloud computing.

Τα οφέλη της τόσο σε οικονομικό όσο και σε κοινωνικό επίπεδο είναι ευρέως αναγνωρισμένα.

- Ένα από τα κύρια οφέλη είναι το γεγονός ότι η εφαρμογή δεν βρίσκεται αποθηκευμένη στο κομπιούτερ μας και έτσι οι όποιες απαιτούμενες αναβαθμίσεις γίνονται αυτόματα και ανέξοδα για τους χρήστες .

- Επιπλέον το γεγονός ότι η εφαρμογή δεν είναι εγκατεστημένη στον κομπιούτερ αλλά βρίσκεται στο διαδίκτυο δίνει μια πολύ μεγάλη ευελιξία καθώς έχουμε άμεση πρόσβαση στην εφαρμογή από οποιαδήποτε συσκευή διαθέτει σύνδεση στο διαδίκτυο

- Ένα ακόμα μεγάλο κέρδος που έχει μια εταιρία , με την χρήση του cloud computing είναι η οικονομία καθώς η αγορά και χρήση ενός λογισμικού είναι μια μεγάλη δαπάνη για την εταιρία , με την χρήση του υπολογιστικού νέφους η εταιρία δεν πληρώνει την αγορά του λογισμικού αλλά μόνο την χρήση της εφαρμογής έτσι το κόστος είναι αρκετά πιο μικρό.
- Τέλος ο μεγάλος αποθηκευτικός χώρος είναι ακόμα ένα μεγάλο πλεονέκτημα, οι καθώς οι εταιρίες μπορούν και έχουν όσο χώρο επιθυμούν χωρίς να βαραίνουν τους υπολογιστές τους.

### 3.4.2 Μειονεκτήματα υπολογιστικού νέφους

Μπορεί τα οφέλη να είναι πολλά και να επιφέρουν μια μεγάλη βοήθεια και ευχέρεια στους χρήστες ωστόσο υπάρχουν και σημαντικά μειονεκτήματα για τα οποία θα πρέπει να είναι γνώστης κάθε χρήστης του υπολογιστικού νέφους .

- Το κυριότερο είναι η έλλειψη του πλήρη ελέγχου καθώς τα δεδομένα διατίθενται από τους χρήστες υπό την διαχείριση των παροχών υπηρεσιών του υπολογιστικού νέφους . Αυτό θα πρέπει να το λάβουν σοβαρά υπόψη και οι εταιρίες που κάνουν χρήση του υπολογιστικού νέφους. Εδώ αναφερόμαστε και στις περιπτώσεις όπου υπάρχει άρση του απορρήτου για νομικούς σκοπούς και η επιβολή γίνεται απευθείας στους παρόχους των υπηρεσιών του υπολογιστικού νέφους .

- Κάτι ακόμα σημαντικό για τις εταιρίες που κάνουν χρήση λογισμικών μέσω cloud είναι ότι εάν μελλοντικά θελήσουν να αλλάξουν πάροχο και να μεταφέρουν τα δεδομένα τους , ενδέχεται να μην είναι εύκολη η φορητότητα των δεδομένων λόγο ασυμβατότητας των μεταξύ εφαρμογών.

- Τέλος υπάρχει και έντονα η αίσθηση της έλλειψης των πληροφοριών όσον αφορά την επεξεργασία που θα υποστούν τα δεδομένα, καθώς οι διαδικασίες επεξεργασίας των δεδομένων που γίνονται στο πλαίσιο των παροχών υπηρεσιών υπολογιστικού νέφους δεν γίνονται πάντα γνωστές στους χρήστες .

### 3.4.3 Μοντέλα ανάπτυξης υπολογιστικού νέφους

Υπάρχουν 4διαφορετικά μοντέλα ανάπτυξης του υπολογιστικού νέφους τα οποία συναντάμε :

- **Ιδιωτικό υπολογιστικό νέφος (Private cloud)** Η cloud υποδομή λειτουργεί αποκλειστικά και μόνο για έναν. Η διαχείρισή της μπορεί να γίνεται από τον ίδιο τον οργανισμό ή από τρίτους και μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων του οργανισμού, και ο οποίος τελεί υπό τον αυστηρό έλεγχο του υπευθύνου της επεξεργασίας.

- **Δημόσιο Υπολογιστικό νέφος (Public cloud):** Η cloud υποδομή ανήκει σε πάροχο που ειδικεύεται στην παροχή υπηρεσιών για χρήστες ή επιχειρήσεις ή ακόμα και για φορείς δημόσιας διοίκησης, η πρόσβαση στις υπηρεσίες είναι μέσω του διαδικτύου, το οποίο σημαίνει ότι υπάρχει μια διαβίβαση των δεδομένων στα συστήματα του παρόχου υπηρεσιών. Έτσι ο πάροχος υπηρεσιών (συνήθως είναι μια εταιρία, η οποία ανήκει σε έναν οργανισμό) έχει μεγάλο ρόλο όσον αφορά την προστασία των δεδομένων .

- **Κοινοτικό υπολογιστικό νέφος (Community cloud):** Όπου η cloud υποδομή της τεχνολογίας των πληροφοριών μοιράζεται μεταξύ πολλών οργανισμών και υποστηρίζει μια συγκεκριμένη κοινότητα που έχει κοινές ανησυχίες (πχ. αποστολή, απαιτήσεις ασφαλείας, πολιτική και θέματα συμμόρφωσης). Η διαχείρισή της μπορεί να γίνεται από τον ίδιο τον οργανισμό ή από τρίτους και μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων του οργανισμού.

- **Υβριδικό υπολογιστικό νέφος (Hybrid cloud):** ή αλλιώς λέγεται και ενδιάμεσο υπολογιστικό νέφος όπου η cloud υποδομή τους είναι μια σύνθεση από υπηρεσίες των δύο ή και περισσότερων υπολογιστικών νέφων και συνήθως συνυπάρχουν οι ιδιωτικές υπηρεσίες από ένα private cloud μαζί υπηρεσίες που κάποιος αγοράζει και κάνει χρήση από δημόσια υπολογιστικά νέφη.

### 3.4.4 Μοντέλα παροχής υπηρεσιών

Υπάρχουν διάφορες λύσεις για το υπολογιστικό νέφος οι οποίες διατίθενται στην αγορά για τους χρήστες :

**1.Υποδομή υπολογιστικού νέφους ως υπηρεσία - Cloud Infrastructure as a Service (IAAS):**

Προσφέρεται η δυνατότητα στον χρήστη να μπορεί να μισθώσει μια τεχνολογική υποδομή με :

1.1. Επεξεργαστική ισχύ

1.2. Αποθηκευτικά μέσα

1.3. Δίκτυα

1.4. Και άλλους θεμελιώδεις υπολογιστικούς πόρους

Τα οποία προσφέρονται στον καταναλωτή από απομακρυσμένους διακομιστές , έτσι αναπτύσσονται από τον χρήστη λειτουργικά εταιρικά συστήματα και άλλες εφαρμογές .

Η διαχείριση και ο έλεγχος της χρησιμοποιούμενης cloud υποδομής βρίσκεται αποκλειστικά στον πάροχο όμως ο έλεγχος των λειτουργικών συστημάτων ,των αποθηκευτικών μέσων και των όποιων εφαρμογών έχουν αναπτυχθεί ανήκει στον καταναλωτή – χρήστη .

**2. Λογισμικό υπολογιστικού νέφους ως υπηρεσία - Cloud Software as a Service (SaaS):**

Προσφέρεται η δυνατότητα στον χρήστη να χρησιμοποιεί τις εφαρμογές του παρόχου που τρέχουν σε μια cloud υποδομή, οι παροχές αυτές προσφέρονται μέσω του παγκόσμιου ιστού και είναι προσβάσιμες από διάφορες client συσκευές ενός thin client interface , τέτοιες εφαρμογές είναι :

2.1. Διάφορα προγράμματα γραφείου μέσω web (τύπου office)

2.2. Εργαλεία επεξεργασίας κειμένου

2.3. Ηλεκτρονικά μητρώα

2.4. Ατζέντες

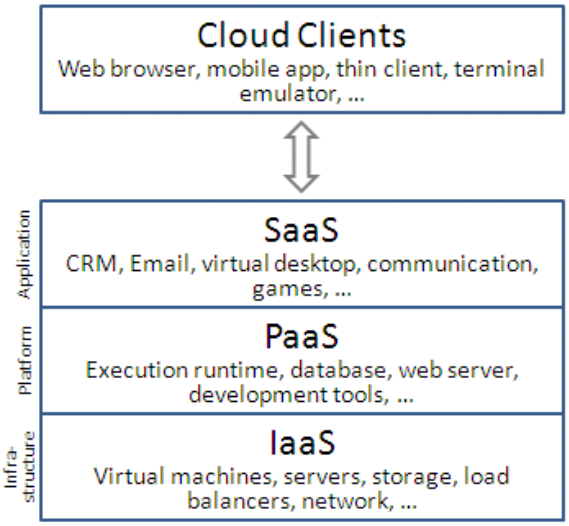
2.5. Ημερολόγια

2.6. E-mail κ.α.

Η διαχείριση και ο έλεγχος της χρησιμοποιούμενης cloud υποδομής βρίσκεται αποκλειστικά στον πάροχο και ο χρήστης έχει μόνο την χρήση των διάφορων εφαρμογών.

**3. Πλατφόρμα υπολογιστικού νέφους ως υπηρεσία - Cloud Platform as a Service (PaaS):**

Προσφέρεται η δυνατότητα στον χρήστη να αναπτύξει πάνω στην cloud δομή διάφορες εφαρμογές, οι οποίες απευθύνονται σε τρίτους , για την κάλυψη εσωτερικών απαιτήσεων σε εταιρίες ή άλλες υπηρεσίες . Η δημιουργία των εφαρμογών δημιουργούνται με όποια γλώσσα προγραμματισμού υποστηρίζει ο πάροχος της δομής cloud. Ο καταναλωτής – χρήστης έχει τον




έλεγχο των εφαρμογών που έχει ο ίδιος αναπτύξει άλλα δεν διαχειρίζεται την υποδομή cloud (δηλαδή τα λειτουργικά συστήματα , servers, τα δίκτυα ) .

## 3.4.5 Νομικό πλαίσιο προστασίας δεδομένων του υπολογιστικού νέφους

Το ισχύον νομικό πλαίσιο είναι η οδηγία 95/46/ΕΚ που αφορά την προστασία των δεδομένων και ισχύει σε κάθε περίπτωση όπου υπάρχει επεξεργασία προσωπικών δεδομένων προσωπικού χαρακτήρα.

Τα πρόσωπα στα οποία αναφέρονται τα δεδομένα προσωπικού χαρακτήρα που υφίσταται επεξεργασία εντός του υπολογιστικού νέφους πρέπει οπωσδήποτε να ενημερώνονται για την

ταυτότητα του υπευθύνου της επεξεργασίας των δεδομένων και για τον σκοπό της επεξεργασίας .
(οι απαιτήσεις αυτές είναι ίδιες για όλους τους υπεύθυνους επεξεργασίας)
Λόγω της ενδεχόμενης πολυπλοκότητας των αλυσιδωτών διαδικασιών επεξεργασίας εντός του εκάστοτε υπολογιστικού νέφους , για να εξασφαλίζεται η θεμιτή επεξεργασία έναντι του προσώπου στο οποίο αναφέρονται τα δεδομένα στο άρθρο 10 της οδηγίας 95/46/ΕΚ [01] οι υπεύθυνοι της επεξεργασίας προτείνεται επίσης, στο πλαίσιο ορθής πρακτικής , να παρέχουν περαιτέρω πληροφορίες σχετικά με τους (υπό-)εκτελούντες την επεξεργασία που παρέχουν τις υπηρεσίες υπολογιστικού νέφους σχετικά με:

α) την ταυτότητα του υπευθύνου της επεξεργασίας και, ενδεχομένως, του εκπροσώπου του-

β) τους σκοπούς της επεξεργασίας για την οποία προορίζονται τα δεδομένα-

γ) οποιαδήποτε περαιτέρω πληροφορία, όπως:

- τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων,
- το κατά πόσον η παροχή των δεδομένων είναι υποχρεωτική ή όχι, καθώς και τις ενδεχόμενες συνέπειες της άρνησης παροχής τους,
- την ύπαρξη δικαιώματος πρόσβασης στα συγκεκριμένα δεδομένα και δικαιώματος διόρθωσής τους,

εφόσον οι πληροφορίες αυτές είναι αναγκαίες, λόγω των ειδικών συνθηκών υπό τις οποίες συλλέγονται τα δεδομένα, ώστε να εξασφαλίζεται η θεμιτή επεξεργασία έναντι του προσώπου στο οποίο αναφέρονται τα δεδομένα.

Σε αυτό το σημείο θα πρέπει να αναφέρουμε και το άρθρο 4 της οδηγίας 95/46 [01] όπου αναφέρονται τα κριτήρια βάση των οποίων προσδιορίζεται το εκάστοτε δίκαιο και αφορά σε όσους παρόχους είναι εγκατεστημένοι εντός ΕΟΧ (Ευρωπαϊκός Οικονομικός Χώρος) και σε όσους παρόχους είναι εγκατεστημένοι εκτός ΕΟΧ που όμως χρησιμοποιούν για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα μέσα εγκατεστημένα εντός ΕΟΧ.

<u>Έτσι σύμφωνα με τον κανονισμό διακρίνουμε τρεις περιπτώσεις :</u>

- **Η πρώτη περίπτωση** αφορά παρόχους υπολογιστικού νέφους οι οποίοι βρίσκονται εγκατεστημένοι εντός ΕΕ , τότε στην περίπτωση αυτή εφαρμόζεται το δίκαιο της χώρας

στην οποία είναι εγκατεστημένος ο υπεύθυνος της επεξεργασίας ,και όχι το δίκαιο της χώρας του παρόχου.

- **Η δεύτερη περίπτωση** αφορά πάλι παρόχους υπολογιστικού νέφους οι οποίοι βρίσκονται εγκατεστημένοι εντός ΕΕ , όμως ο υπεύθυνος της επεξεργασίας είναι εγκατεστημένος σε περισσότερα από ένα κράτη μέλη τότε είναι υποχρεωμένος να εφαρμόζει το δίκαιο καθενός ξεχωριστά εκ των κρατών μελών στο οποίο λαμβάνει χώρα η εν λόγω επεξεργασία.

- **Η Τρίτη περίπτωση** αφορά τους υπευθύνους επεξεργασίας οι οποίοι δεν είναι εγκατεστημένοι εντός ΕΕ αλλά έχει προσλάβει πάροχο υπηρεσιών υπολογιστικού νέφους εγκατεστημένο εντός του ΕΕ, έτσι η νομοθεσία που υπάρχει στον πάροχο αφορά και τον πελάτη και υποχρεούται να συμμορφώνεται σύμφωνα με το δίκαιο του κράτους στο οποίο ανήκει.

Αναλύοντας τις τρεις αυτές περιπτώσεις κατανοούμε ότι υπάρχει μια στενή σχέση ευθυνών ανάμεσα στον πάροχο υπηρεσιών και τον υπεύθυνο επεξεργασίας των δεδομένων .
Ο πάροχος υπηρεσιών υπολογιστικού νέφους είναι η οντότητα που παρέχει τις υπηρεσίες υπολογιστικού νέφους , ενώ ο υπεύθυνος επεξεργασίας είναι αυτός όπου καθορίζει τους στόχους και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.
Είναι και οι δύο υπόλογοι όσο αφορά την σωστή και νόμιμη λειτουργία του cloud ,και κυρίως την διασφάλιση του απορρήτου των προσωπικών δεδομένων έτσι θα πρέπει όλες οι υποχρεώσεις συμμόρφωσης προς τους κανόνες των δεδομένων και οι ευθύνες σε περίπτωση πιθανής παραβίασης τους πρέπει να κατανέμονται με σαφήνεια ώστε να διατηρείται πάντα το επίπεδο ασφαλείας των δεδομένων σε ψηλά επίπεδα.

Οι πελάτες του υπολογιστικού νέφους συνήθως δεν έχουν περιθώρια διαπραγμάτευσης καθώς οι πιο πολλές υπηρεσίες υπολογιστικού νέφους χρησιμοποιούν τυποποιημένες συμβάσεις και ο πελάτης υποχρεούται να αποδεχθεί την σύμβαση για να κάνει χρήση της εφαρμογής.

Ωστόσο κάθε πελάτης πριν προβεί στην χρήση μια υπηρεσίας cloud θα πρέπει να βεβαιωθεί ότι η υπηρεσία στην οποία πρόκειται να ανάθεση τα προσωπικά του δεδομένα έχει τα εξής κύρια χαρακτηριστικά :

1. Συμμόρφωση προς τις βασικές αρχές της νομοθεσίας της ΕΕ .

2. Διαφάνεια έναντι του προσώπου στο οποίο αναφέρονται τα δεδομένα
3. Να τηρείται η αρχή του προσδιορισμού και του περιορισμού του σκοπού
4. Και τέλος να διαγράφονται τα δεδομένα προσωπικού χαρακτήρα μόλις πάψει να είναι πλέον απαραίτητη η διατήρησή τους.

### 3.4.6 Φορητότητα

Ακόμα κάτι σημαντικό που θα πρέπει κυρίως ο πελάτης να ελέγχει είναι η δυνατότητα της φορητότητας των δεδομένων καθώς οι περισσότεροι πάροχοι υπηρεσιών υπολογιστικού νέφους δεν κάνουν χρήση τυποποιημένων μορφότυπων δεδομένων και διεπαφών υπηρεσιών που να διευκολύνουν τη διαλειτουργικότητα και την φορητότητα μεταξύ των διαφόρων παρόχων υπηρεσιών υπολογιστικού νέφους . Έτσι στην περίπτωση που ο πελάτης θελήσει να αλλάξει τον πάροχο της νεφουπολογιστικής υπηρεσίας που χρησιμοποιεί θα βρεθεί στην δυσάρεστη θέση της αδυναμίας της μεταφοράς των δεδομένων του στο νέο πάροχο. Κάτι αντίστοιχο ισχύει και για τις υπηρεσίες που ενδεχομένως έχει αναπτύξει ο ίδιος ο πελάτης μέσα σε μια δομή cloud , σε περίπτωση που θελήσει να αλλάξει πάροχο υπηρεσιών τότε η μεταφορά είναι από δύσκολη έως αδύνατον.

# Κεφάλαιο 4

# Σχέδιο νέου Κανονισμού για την προστασία προσωπικών δεδομένων

Στο κεφάλαιο αυτό παρουσιάζονται οι κύριες αλλαγές που θα επιφέρει ο Νέος Κανονισμός του Ευρωπαϊκού Κοινοβουλίου για την προστασία των προσωπικών δεδομένων, ο οποίος θα αντικαταστήσει το υπάρχον νομικό πλαίσιο. (Οδηγία 95/46/ΕΚ).

Με την συγκρότηση του ενιαίου ευρωπαίου χώρου την 1η Νοεμβρίου 1993, δημιουργήθηκε μια οικονομική και πολιτική ένωση που πλέον αριθμεί 27 κράτη μέλη με κοινό όραμα και κοινούς στόχους , την ενωμένη Ευρώπη. Κατά την πάροδο των χρόνων έχουν γίνει πολλές τροποιητικές συνθήκες με πρωταρχικό όραμα μια Ευρώπη ενωμένης σε όλα τα επίπεδα και ιδίως μιας ενιαίας Ευρώπης χωρίς σύνορα μεταξύ των κρατών μελών. Σήμερα βρισκόμαστε μπροστά σε μια ακόμα μεγάλη αλλαγή, στη θέσπιση ενός ενιαίου δεσμευτικού νομικού πλαισίου για την προστασία των προσωπικών δεδομένων, η οποία θα επιφέρει την πλήρη ενοποίηση του δικαίου σε αυτόν τον τομέα.

# 4.1.Ενιαίο πλέγμα κανόνων

Μέχρι σήμερα τα 27 κράτη μέλη της ΕΕ έχουν εφαρμόσει τους ευρωπαϊκούς κανόνες με μικρές μεν αλλά υπαρκτές δε αποκλίσεις οι οποίες , επιφέρουν το αποτέλεσμα ενός ανομοιογενούς πλαισίου. Αυτό οφείλεται στο γεγονός ότι η νομική φύση των ευρωπαϊκών Οδηγιών επιτρέπει πάντα μία ευελιξία στον τρόπο με τον οποίο αυτές θα ενσωματωθούν στην έννομη τάξη κάθε χώρας, (για παράδειγμα, ο ν. 2472/1997 για την προστασία των προσωπικών δεδομένων στην Ελλάδα ενσωματώνει μεν την ευρωπαϊκή Οδηγία 95/46/ΕΚ, αλλά αφενός δεν ταυτίζεται πλήρως με αυτή σε όλα τα επίπεδα, αφετέρου διαφέρει σε επιμέρους ζητήματα από την αντίστοιχη νομοθεσία άλλων ευρωπαϊκών χωρών που έχουν επίσης ενσωματώσει την ίδια Οδηγία).

Σε αυτό το σημείο πρέπει να τονίσουμε την ιδιαιτερότητα της Ευρωπαϊκής Νομοθεσίας, η οποία, είτε είναι διατυπωμένη με την μορφή οδηγιών, ( όπου υπάρχει η υποχρέωση ενσωμάτωσης τους, δηλαδή υποχρέωση ως προς το αποτέλεσμα της οδηγίας) είτε με την μορφή κανονισμών

(όπου υπάρχει η υποχρέωση εφαρμογής τους) πρέπει σε κάθε περίπτωση να εφαρμόζονται υπό το φως και με βάση τις αρχές του Ευρωπαϊκού Δικαίου, και σύμφωνα με την ερμηνεία των Ευρωπαικών Δικαστηρίων, δηλαδή σε κάθε περίπτωση που ο Έλληνας δικαστής – εφαρμοστής του Ευρωπαικού Δικαίου έχει κάποια αμφιβολία πρέπει να ανατρέχει στην νομολογία των Ευρωπαικών Δικαστηρίων, ενώ το δικαστήριο σε περίπτωση αμφιβολίας ως προς την ερμηνεία του Ευρωπαϊκού Δικαίου μπορεί ή και υποχρεούται σε κάποιες περιπτώσεις να διατυπώσει προδικαστικό ερώτημα στο Δικαστήριο της Ευρωπαϊκής Ένωσης.

Ως εκ τούτου, θεωρείται πλέον αναγκαία η εφαρμογή ενός νέου Κανονισμού με κοινή εφαρμογή σε όλα τα κράτη μέλη που θα αντικαταστήσει την εθνική νομοθεσία. Στο άρθρο 38 του Νέου κανονισμού προτείνεται να καθιερωθεί μια ενιαία νομοθεσία η οποία θα εφαρμόζεται αλλά και με την χρήση κωδικών δεοντολογίας αποσκοπώντας την ορθή και κοινή εφαρμογή σε όλα τα κράτη μέλη.

Λαμβάνοντας υπόψη τα ειδικά χαρακτηριστικά των διάφορων τομέων επεξεργασίας δεδομένων επισημαίνονται μερικά επιγραμματικά χαρακτηριστικά που θα αναλυθούν από τους κώδικες δεοντολογίας :

α) Τη θεμιτή και διαφανή επεξεργασία των δεδομένων·

β) Τη συλλογή δεδομένων·

γ) Την ενημέρωση του κοινού και των προσώπων στα οποία αναφέρονται τα δεδομένα·

δ) Τα αιτήματα των προσώπων στα οποία αναφέρονται τα δεδομένα κατά την άσκηση των δικαιωμάτων τους·

ε) Την ενημέρωση και την προστασία των παιδιών·

στ) Τη διαβίβαση δεδομένων σε τρίτες χώρες ή διεθνείς οργανισμούς·

ζ) Τους μηχανισμούς παρακολούθησης και διασφάλισης της συμμόρφωσης προς τον κώδικα από τους υπευθύνους επεξεργασίας που τον εφαρμόζουν

.

(Η έννοια του κώδικα δεοντολογίας εμφανίζεται στο άρθρο 27 παράγραφος 1 της οδηγίας 95/46/[ΕΚ]) [01]

## 4.2. Ύπαρξη μοναδικής εθνικής αρχής προστασίας για την προστασία των δεδομένων .

Πέρα από το ενιαίο πλέγμα κανόνων, στο σχέδιο του νέου Κανονισμού προτείνεται μια μόνο εθνική αρχή για την προστασία των δεδομένων, η οποία και θα επιφορτίζεται το βάρος της παρακολούθησης του νέου Κανονισμού και επιπλέον θα συμβάλλει στη συνεκτική εφαρμογή του σε ολόκληρη την 'Ευρωπαϊκή Ένωση.

Όλες οι εταιρίες και όλοι οι χρήστες του ίντερνετ θα είναι υπόλογοι σε ότι αφορά τα προσωπικά δεδομένα σε αυτήν, περαιτέρω η αρχή αυτή θα είναι υπεύθυνη για κάθε επιχείρηση που έχει έδρα στη χώρα της.

Μέχρι σήμερα υπάρχουν 27 διαφορετικές εθνικές νομοθεσίες που αφορούν την προστασία των προσωπικών δεδομένων. Αυτή η διάσπαρτη νομοθεσία δυσκολεύει την πρόσβαση των εταιρειών σε νέες αγορές και παράλληλα δεν αποτρέπει αποτελεσματικά κακόβουλα άτομα στο να αποσπούν προσωπικά δεδομένα.

Πλέον κάθε εταιρία θα είναι υπόλογη μόνο σε μια αρχή προστασία προσωπικών δεδομένων, της χώρας στην οποία βρίσκεται η έδρα της εταιρίας. Παράλληλα ωστόσο η εταιρεία θα μπορεί να δραστηριοποιείται σε όλες της χώρες της ευρωπαϊκής ένωσης. Αυτό έχει μέγιστο θετικό αποτέλεσμα καθώς σε μια εποχή όπου πολλά κράτη της Ευρώπης μαστίζονται από την κρίση οι επιχειρήσεις, θα μπορούν να απευθύνονται σε πολύ μεγαλύτερο αγοραστικό κοινό. Τόσο οι επιχειρήσεις όσο και οι καταναλωτές θα έχουν πλέον ένα ενιαίο σημείο επαφής.

Παρομοίως και οι πολίτες θα μπορούν να απευθύνονται στην αρχή προστασία δεδομένων της χώρας τους , ακόμα και στην περίπτωση που τα δεδομένα τους υποβάλλονται σε επεξεργασία εκτός της ΕΕ. (κάτι το οποίο μέχρι τώρα δεν συμβαίνει, δυσχεραίνοντας την προστασία των προσώπων από παράνομη επεξεργασία των δεδομένων – βλέπε και την Γνώμη 8/2010 της Ομάδας Εργασίας του Άρθρου 29 για το εφαρμοστέο δίκαιο: [25]

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_el.pdf

Για παράδειγμα, με το υπάρχον νομικό πλαίσιο, για τυχόν παράνομη επεξεργασία προσωπικών δεδομένων έλληνα χρήστη από το Google, η ελληνική αρχή προστασίας προσωπικών δεδομένων δεν έχει – κατ' αρχήν – αρμοδιότητα να επιληφθεί.

Εδώ θα πρέπει να διευκρινίσουμε ότι η αρχή ελέγχου δεν είναι αρμόδια να εποπτεύει τις πράξεις επεξεργασίας από δικαστήρια τα οποία ενεργούν στο πλαίσιο της δικαιοδοτικής τους ιδιότητας.

(Τα παραπάνω αναφέρονται στα άρθρα 46-52 του Νέου Κανονισμού )

## 4.3 Συγκατάθεση

Μέχρι σήμερα ο ορισμός της «συγκατάθεσης» δίνεται από τον ελληνικό, νόμο 2472/1997, άρθρο 2) και το κοινοτικό δίκαιο ως :

«Κάθε δήλωση βούλησης, ελεύθερης, ρητής και εν πλήρη επίγνωση, με την οποία το πρόσωπο στο οποίο αναφέρονται τα δεδομένα δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν»

Και επιπλέον ορίζεται και στο άρθρο 2 της οδηγίας 95/46/ΕΚ. : «Κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή, και εν πλήρη επίγνωση, και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Η ενημέρωση αυτή περιλαμβάνει πληροφόρηση τουλάχιστον για τον σκοπό της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, καθώς και το όνομα, την επωνυμία και τη διεύθυνση του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου του. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα.»

Κατά συνέπεια, η συγκατάθεση κατά την έννοια της οδηγίας 95/46 , ισοδυναμεί με συγκατάθεση του χρήστη κατόπιν πλήρους ενημέρωσής του, το οποίο είναι και ένα πολύ βασικό στοιχείο του δικαιώματος της πληροφοριακής αυτοδιάθεσης (δηλ, η δυνατότητα του ατόμου στο να γνωρίζει, να παρακολουθεί και να ελέγχει ποιος και γιατί συλλέγει και διατηρεί πληροφορίες που τον αφορούν). Εξάλλου, και η ελληνική αρχή προστασίας προσωπικών

δεδομένων έχει κρίνει σε διάφορες περιπτώσεις ότι, προκειμένου τα φυσικά πρόσωπα να παρέχουν την ελεύθερη, ρητή και ειδική συγκατάθεσή τους για μία επεξεργασία, απαιτείται να έχουν προηγουμένως ενημερωθεί για τα βασικά στοιχεία αυτής (βλ. π.χ. Γνωμοδότηση 4/2010 της Αρχής αναφορικά με την κάρτα αποδείξεων, διαθέσιμη στο διαδικτυακό της τόπο www.dpa.gr ).

Η έννοια της πλήρους ενημέρωσης ωστόσο είναι ιδιάζουσας σημασίας συχνά υπάρχει μια έντονη αμφισβήτηση από την πλευρά των χρηστών καθώς οι δηλώσεις ιδιωτικότητας («privacy statements») και οι γενικοί όροι των προϋποθέσεων χρήσης είναι δύσκολο να κατανοηθούν από τον χρήστη (ενώ πολλές φορές οι όροι χρήσης δεν είναι καν σε ευκρινές σημείο) περαιτέρω, είναι συχνό το φαινόμενο να πρέπει ένας χρήστης, προκειμένου να μπορέσει να χρησιμοποιήσει μια υπηρεσία να κάνει αποδοχή των όρων χρήσης, - με άλλα λόγια, πρέπει αναγκαστικά να δώσει την συγκατάθεση του στου όρους της εφαρμογής, κάτι το οποίο δεν μπορεί σε καμία περίπτωση να εκληφθεί ως ελεύθερη συγκατάθεση.

Ο νέος κανονισμός έρχεται να δώσει μια κύρια αλλαγή στην έννοια της συγκατάθεσης η οποία θα είναι:

«Όταν απαιτείται συγκατάθεση για τη διαχείριση δεδομένων, αυτή θα πρέπει να δίδεται ρητά, και όχι να λαμβάνεται ως δεδομένη»

Η ρητή και σαφής συγκατάθεση είναι ένα ακόμα λιθαράκι στην επίτευξη του «τοίχους» προστασίας των προσωπικών δεδομένων των πολιτών . Επίσης, με το νέο σχέδιο του κανονισμού, η απαίτηση για ρητή ενημέρωση προ της συγκατάθεσης διατηρείται.

Επιπλέον, όταν υπάρχει μια σημαντική ανισοβαρής σχέση μεταξύ της θέσης του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας (τυπική τέτοια περίπτωση είναι οι σχέσεις εργαζομένου και εργοδότη), η συγκατάθεση δεν μπορεί να αποτελέσει νομική βάση για την επεξεργασία. Η σύζευξη της χρήσης της υπηρεσίας με την χρήση προσωπικών δεδομένων, απαγορεύεται ακόμη και αν η χρήση επεκτείνεται πέρα από την άμεση αλληλεπίδραση πελάτη υπηρεσίας.

Οι επιχειρήσεις θα μπορούν να επεξεργασθούν τα στοιχεία μόνον αφού λάβουν προς τούτο τη συγκατάθεση των χρηστών ενώ ο εισηγητής του [ΕΚ] Γιαν Φίλιπ Άλμπρεχτ θέλει να προστεθεί ειδική πρόνοια πώς η συγκατάθεση θα ισχύσει για συγκεκριμένη χρήση και θα πρέπει να ανανεώνεται για κάθε πρόσθετη «αξιοποίηση» των στοιχείων. [37]

Ο Νέος κανονισμός αναφέρει στο άρθρο 7 τις προϋποθέσεις της συγκατάθεσης:

1. Ο υπεύθυνος επεξεργασίας φέρει το βάρος της απόδειξης όσον αφορά την παροχή της συγκατάθεσης του προσώπου στο οποίο αναφέρονται τα δεδομένα στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν για συγκεκριμένους σκοπούς.

2. Εάν η συγκατάθεση του προσώπου στο οποίο αναφέρονται τα δεδομένα παρέχεται στο πλαίσιο έγγραφης δήλωσης η οποία αφορά και άλλο θέμα, η απαίτηση παροχής συγκατάθεσης πρέπει να είναι διακριτή σε σχέση με το εν λόγω άλλο θέμα.

3. Το πρόσωπο στο οποίο αναφέρονται τα δεδομένα δικαιούται να αποσύρει τη συγκατάθεσή του ανά πάσα στιγμή. Η απόσυρση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίσθηκε στη συγκατάθεση προ της απόσυρσής της.»

## 4.4 Γνωστοποίηση περιστατικών παραβίαση δεδομένων

Με την βελτίωση των κανόνων προστασίας των δεδομένων θα υπάρξει θα υπάρξει μεγαλύτερη ασφάλεια όσον αφορά τη διαχείριση των προσωπικών δεδομένων, ιδιαίτερα στο διαδίκτυο. Οι ισχυρότεροι κανόνες προστασίας δεδομένων θα ενισχύσουν την εμπιστοσύνη στις διαδικτυακές υπηρεσίες, και ως εκ τούτου οι νέες τεχνολογίες θα χρησιμοποιούνται με μεγαλύτερη σιγουριά, αξιοποιώντας τα πλεονεκτήματα της εσωτερικής αγοράς. Οι νέοι, σαφείς και αυστηροί κανόνες για την ελεύθερη κυκλοφορία δεδομένων θα βοηθήσουν επίσης τις επιχειρήσεις να αναπτυχθούν μέσα σε ένα αξιόπιστο πλαίσιο προστασίας δεδομένων, με αποτέλεσμα να διευκολυνθεί η πρόσβαση σε περισσότερα αγαθά και υπηρεσίες σε καλύτερες τιμές.

Ένας από τους νέους κανόνες που αλλάζει αφορά εταιρείες και οργανισμούς, και έρχεται να επεκτείνει την αυστηρότητα για την προστασία των προσωπικών δεδομένων που μέχρι τώρα όριζε το άρθρο 30 της οδηγίας 95/46/ΕΚ. Συγκεκριμένα, στην υπάρχουσα Οδηγία αναφέρεται το εξής: :

2. Τα κράτη μέλη μπορούν να προσδιορίζουν τις προϋποθέσεις υπό τις οποίες τα δεδομένα προσωπικού χαρακτήρα μπορούν να χρησιμοποιούνται και να ανακοινώνονται σε τρίτους στα πλαίσια νόμιμης συνήθους δραστηριότητας στις επιχειρήσεις ή άλλους οργανισμούς- επίσης μπορούν να προσδιορίζουν τις προϋποθέσεις υπό τις οποίες μπορούν να ανακοινώνονται σε τρίτους τα δεδομένα προσωπικού χαρακτήρα για εμπορικούς ή διαφημιστικούς σκοπούς που επιδιώκονται είτε από εμπορικούς φορείς είτε από φιλανθρωπικά σωματεία ή άλλες οργανώσεις ή ενώσεις, λ.χ. πολιτικού χαρακτήρα, με την επιφύλαξη των διατάξεων που επιτρέπουν στα πρόσωπα στα οποία αναφέρονται τα δεδομένα να αντιταχθούν χωρίς αιτιολόγηση και άνευ δαπάνης στην επεξεργασία των δεδομένων που τα αφορούν-

Με τον νέο κανονισμό πλέον, όλοι οι φορείς (εταιρείες, και οι οργανισμοί κτλ.) θα υποχρεούνται να γνωστοποιούν τις σοβαρές παραβιάσεις δεδομένων που λαμβάνουν χώρα χωρίς καθυστέρηση, και, εφόσον είναι εφικτό, εντός 24 ωρών. Με λίγα λόγια οφείλουν να γνωστοποιούν παραβιάσεις των προσωπικών δεδομένων που θα μπορούσαν να είναι επιζήμιες για τους χρήστες του ιντερνέτ καθώς επίσης πρέπει να ενημερώνουν σχετικά και την αρμόδια αρχή προστασίας δεδομένων.

Η ακριβής διατύπωση του άρθρου 67 του νέου κανονισμού είναι η εξής :

- Η παραβίαση δεδομένων προσωπικού χαρακτήρα μπορεί, εάν δεν αντιμετωπισθεί κατάλληλα και έγκαιρα, να έχει ως αποτέλεσμα σημαντική οικονομική ζημία και κοινωνική βλάβη -συμπεριλαμβανομένης της υποκλοπής ταυτότητας- για το ενδιαφερόμενο φυσικό πρόσωπο. Επομένως, μόλις ο υπεύθυνος επεξεργασίας αντιληφθεί μια τέτοια παραβίαση, πρέπει να γνωστοποιήσει την παραβίαση στην αρχή ελέγχου αμελλητί και, ει δυνατόν, εντός 24 ωρών. Εάν αυτό δεν μπορεί να επιτευχθεί εντός 24 ωρών, η γνωστοποίηση πρέπει να συνοδεύεται από αιτιολογία η οποία αναφέρει τους λόγους της καθυστέρησης. Τα φυσικά πρόσωπα των οποίων τα δεδομένα προσωπικού χαρακτήρα μπορεί να επηρεασθούν αρνητικά από την παραβίαση πρέπει να ενημερώνονται αμελλητί προκειμένου να μπορούν να λάβουν τις αναγκαίες προφυλάξεις. Η παραβίαση πρέπει να θεωρείται ότι επηρεάζει αρνητικά τα δεδομένα προσωπικού χαρακτήρα ή την ιδιωτική ζωή

του προσώπου στο οποίο αναφέρονται εάν μπορεί να έχει ως αποτέλεσμα, για παράδειγμα, κατάχρηση ή υποκλοπή ταυτότητας, σωματική βλάβη, σημαντική προσβολή ή βλάβη της φήμης του. Η γνωστοποίηση πρέπει να περιγράφει τη φύση της παραβίασης των δεδομένων προσωπικού χαρακτήρα και να περιέχει συστάσεις προς το ενδιαφερόμενο φυσικό πρόσωπο για τον μετριασμό δυνητικών δυσμενών συνεπειών. Οι γνωστοποιήσεις στα πρόσωπα στα οποία αναφέρονται τα δεδομένα πρέπει να πραγματοποιούνται το συντομότερο δυνατόν, σε στενή συνεργασία με την αρχή ελέγχου και τηρώντας την καθοδήγηση που παρέχεται από αυτήν ή άλλες σχετικές αρχές (π.χ. αρχές επιβολής του νόμου). Για παράδειγμα, η δυνατότητα των προσώπων στα οποία αναφέρονται τα δεδομένα να μετριάσουν έναν άμεσο κίνδυνο βλάβης απαιτεί την άμεση ενημέρωση των προσώπων στα οποία αναφέρονται τα δεδομένα, ενώ η αναγκαιότητα εφαρμογής κατάλληλων μέτρων κατά της συνέχισης της παραβίασης ή άλλων παρόμοιων παραβιάσεων δεδομένων μπορεί να δικαιολογεί μεγαλύτερη καθυστέρηση.

## 4.5 Φορητότητα δεδομένων

Μία σημαντική καινοτομία που προβλέπει ο νέος κανονισμός είναι η θέσπιση του δικαιώματος της φορητότητας των δεδομένων, δηλαδή της εύκολης μεταφοράς των προσωπικών δεδομένων των χρηστών από έναν πάροχο υπηρεσιών σε έναν άλλον. Η πρόβλεψη αυτή υπάρχει στο άρθρο 18 του σχεδίου του κανονισμού: πλέον ο υπεύθυνος επεξεργασίας δεν θα μπορεί να παρεμποδίζει τη φορητότητα των δεδομένων, δηλαδή τη μεταφορά δεδομένων από ένα ηλεκτρονικό σύστημα επεξεργασίας σε ένα άλλο.

Ως προϋπόθεση και για την περαιτέρω βελτίωση της πρόσβασης των φυσικών προσώπων στα δεδομένα προσωπικού χαρακτήρα που τα αφορούν, προβλέπει το δικαίωμα εξασφάλισης των εν λόγω δεδομένων από τον υπεύθυνο επεξεργασίας σε δομημένο και ευρέως χρησιμοποιούμενο ηλεκτρονικό μορφότυπο.

Ειδικότερα στο Άρθρο 18 του νεου κανονισμού αναφέρεται ότι :

[Ο παρών κανονισμός επιτρέπει να λαμβάνεται υπόψη η αρχή της πρόσβασης του κοινού στα επίσημα έγγραφα κατά την εφαρμογή των διατάξεων που προβλέπονται στον παρόντα κανονισμό].

Με την κατοχύρωση του δικαιώματος της φορητότητας, οι χρήστες θα μπορούν να χρησιμοποιούν με ασφάλεια το διαδίκτυο και να αξιοποιούν τις νέες τεχνολογίες ανεξάρτητα από τον τόπο προέλευσής τους, είτε για να πραγματοποιούν συμφέρουσες αγορές είτε για να ανταλλάσσουν πληροφορίες με φίλους σε όλο τον κόσμο. Αυτή η ενισχυμένη εμπιστοσύνη θα συμβάλει επίσης στην ανάπτυξη των επιχειρήσεων δίνοντάς τους τη δυνατότητα να εξυπηρετούν τους πελάτες τους ανά την Ευρώπη με επαρκείς διασφαλίσεις για τα δεδομένα προσωπικού χαρακτήρα και με μικρότερο κόστος.

## 4.6 Δικαίωμα στη λήθη

Μία ακόμα από τις προτάσεις του νέου κανονισμού, η οποία είναι ιδιαίτερα σημαντική και αποτελεί ξεχωριστή καινοτομία, είναι το δικαίωμα στην λήθη (right to be Forgotten). Η πρόταση αυτή αποτελεί γενίκευση του άρθρου 12 του κανονισμού της ευρωπαϊκής οδηγίας 95/46.

Με το δικαίωμα στην λήθη οι χρήστες του διαδικτύου θα μπορούν να διαγράφουν τα προσωπικά τους δεδομένα , τα οποία προέκυψαν από δική τους δραστηριότητα στο παρελθόν.

Συγκεκριμένα αναφέρεται το άρθρο 17 του σχεδίου του νέου κανονισμού, το δικαίωμα των φυσικών προσώπων «να λησμονηθούν» και δικαίωμα διαγραφής :

[Το πρόσωπο στο οποίο αναφέρονται τα δεδομένα δικαιούται να απαιτήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν και τη μη περαιτέρω διάδοση των εν λόγω δεδομένων, ιδίως σε σχέση με δεδομένα προσωπικού χαρακτήρα τα οποία διατέθηκαν από το συγκεκριμένο πρόσωπο κατά την παιδική του ηλικία, εάν συντρέχει ένας από τους ακόλουθους λόγους:

α) Τα δεδομένα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν άλλως πως σε επεξεργασία·

β) Το πρόσωπο στο οποίο αναφέρονται τα δεδομένα αποσύρει τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α), ή εάν το χρονικό διάστημα αποθήκευσης για το οποίο παρασχέθηκε συγκατάθεση έληξε, και εάν δεν υπάρχει άλλος νομικός λόγος για την επεξεργασία των δεδομένων·

γ) Το πρόσωπο στο οποίο αναφέρονται τα δεδομένα αντιτάσσεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα δυνάμει του άρθρου 19·

δ) Η επεξεργασία των δεδομένων δεν είναι σύμφωνη προς τον παρόντα κανονισμό για άλλους λόγους.]

Το δικαίωμα στη λήθη υπόκειται για την ώρα μόνο σε ερμηνείες του κανονισμού καθώς δεν έχει ακόμα διευκρινιστεί πλήρως το νέο κανονιστικό πλαίσιο, και πρέπει να συμφιλιώσουμε δυο αντικρουόμενες έννοιες : την ελευθερία της έκφρασης και το δικαίωμα της λήθης. Για παράδειγμα, το να διαγράψει κάποιος μία ανάρτησή του σε ένα ιστολόγο (blog), παρόλο που είναι σύμφωνο με το ανωτέρω δικαίωμα στη λήθη, ενδεχομένως προσκρούει σε άλλες διατάξεις (χωρίς να συνυπολογίζει κανείς τα πρακτικά ζητήματα που ανακύπτουν).

Για την καλύτερη εφαρμογή των κανόνων εναπόκειται τα δικαστήρια να ερμηνεύσουν το νόμο με τρόπους που αρμόζουν σε συγκεκριμένες περιπτώσεις και να εξελιχθεί η νομολογία καθώς εμφανίζονται νέες εφαρμογές, προϊόντα και σενάρια.

Ωστόσο αυτό που θα πρέπει να γίνει σαφές είναι η μέγιστη προσπάθεια της ευρωπαϊκής ένωσης για να υπάρξει ένα θεμελιώδες δικαίωμα το οποίο θα είναι ενιαίο σε όλα τα κράτη μέλη.

## 4.7 Νέοι Ορισμοί

Στην πρώτη παράγραφο του άρθρου 17 (του νέου κανονισμού) αναφέρεται το «υποκείμενο των δεδομένων» ως «πρόσωπο»

[Το πρόσωπο στο οποίο αναφέρονται τα δεδομένα δικαιούται να απαιτήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν και τη μη περαιτέρω διάδοση των εν λόγω δεδομένων.]

Ο νέος ορισμός του κανονισμού για το υποκείμενο των δεδομένων αναφέρει στο άρθρο 4 ότι το «πρόσωπο στο οποίο αναφέρονται τα δεδομένα» είναι ένα φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, με μέσα τα οποία είναι εύλογα πιθανό να χρησιμοποιηθούν από τον υπεύθυνο επεξεργασίας ή από οποιοδήποτε άλλο φυσικό ή νομικό πρόσωπο, ιδίως βάσει αριθμού ταυτότητας, δεδομένων θέσης, επιγραμμικού αναγνωριστικού ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόσταση του συγκεκριμένου προσώπου από φυσική, βιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη προσώπου από φυσική, βιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη.

Ως δεδομένα προσωπικού χαρακτήρα αναφέρονται (στο ίδιο άρθρο): κάθε πληροφορία η οποία αναφέρεται σε συγκεκριμένο φυσικό πρόσωπο «δηλ. το υποκείμενο των δεδομένων».

# Κεφάλαιο 5

## Η εφαρμογή του νέου κανονισμού στο διαδίκτυο: ανοιχτά ζητήματα

Ο νέος κανονισμός είναι ένα μεγάλο βήμα, για τον τομέα της πληροφορικής. Είναι η αναγκαία εξέλιξη στο θέμα του ιντερνέτ, το διαδικτυακό μέλλον της Ευρώπης, ωστόσο υπάρχουν μερικά σημεία στα οποία αξίζει να δώσει κανείς μια πιο εύλογη σημασία και να τα δούμε λιγάκι εκτενέστερα. Σαφώς οι εγγυήσεις και οι λύσεις που προτείνονται στο κανονισμό είναι τόσο νομικά όσο και τεχνολογικά καταρτισμένες για την προστασία των προσωπικών δεδομένων στον ιντερνέτ. Ωστόσο ο χαρακτήρας της πληροφορικής είναι τόσο πολύπλοκος που καμιά φορά όσο και εάν ένα θέμα το έχεις αναλύσει πάντα υπάρχει ένα μικρό «παραθυράκι» που υπονομεύει έναν μεγάλο «κίνδυνο».

## 5.1 Νέος κανονισμός και υπολογιστικό νέφος

Τα ζητήματα προστασίας προσωπικών δεδομένων που ανακύπτουν σε περιβάλλοντα υπολογιστικού νέφους είναι σημαντικά, λόγω ακριβώς των ιδιαίτερων χαρακτηριστικών αυτής της τεχνολογίας (βλ. επίσης και Γνώμη 5/2012 της Ομάδας Εργασίας του άρθρου 29). Οι δύο κύριοι προβληματισμοί που ανακύπτουν, για οποιαδήποτε δομή υπολογιστικού νέφους, είναι οι εξής:

i. Κατά πόσον ασφαλές είναι σε έναν ο χρήστη του νέφους να αναθέσει την ασφάλεια των προσωπικών δεδομένων σε έναν πάροχο υπηρεσιών υπολογιστικού νέφους,

ii. Εάν τα δεδομένα του χρήστη παραμένουν ασφαλή ακόμα και στην περίπτωση όπου η αποθήκευση τους γίνεται σε χώρα εκτός της Ευρωπαϊκής Ένωσης ;

Κατά συνέπεια, το καίριο ερώτημα είναι να διερευνηθεί κατά πόσον η προτεινόμενη ρύθμιση του νέο κανονισμού θα επιφέρει μεγαλύτερη ασφάλεια τόσο από τεχνολογική όσο και από νομική πλευρά. Στην υπάρχουσα Οδηγία, υπάρχει έντονη η διάκριση μεταξύ του υπεύθυνου επεξεργασίας και του εκτελούντος αυτήν.

Η κύρια ευθύνη συνήθως βαραίνει τον υπεύθυνο επεξεργασίας , ενώ ο εκτελών δεν είναι επιφορτισμένος με άλλες υποχρεώσεις πέραν της υποχρέωσης συμμόρφωσής του με τις συμβατικές υποχρεώσεις του με τον υπεύθυνο επεξεργασίας.

Με τον νέο κανονισμό οι όροι του «υπεύθυνου της επεξεργασία» και του «εκτελούντος την επεξεργασία» παραμένουν . Ωστόσο, με τον νέο κανονισμό της προστασίας των προσωπικών δεδομένων έχουν και οι δύο την ευθύνη για την ασφαλή και νόμιμη επεξεργασία των δεδομένων , και είναι και οι δύο υπεύθυνοι για να λάβουν τα κατάλληλα τεχνολογικά μέτρα ώστε να υπάρχει η διασφάλιση των δεδομένων.

- [Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα ώστε να διασφαλίσουν επίπεδο προστασίας κατάλληλο προς τους κινδύνους που αντιπροσωπεύει η επεξεργασία και η φύση των δεδομένων προσωπικού χαρακτήρα που πρέπει να προστατευθούν, λαμβάνοντας υπόψη την κατάσταση της τεχνολογίας και το κόστος της εφαρμογής τους. Ασφάλεια επεξεργασίας, Άρθρο 30, Νέος Κανονισμός ] [2]

Επιπλέον η συγκεκριμένη υποχρέωση επεκτείνεται και στους εκτελούντες την επεξεργασία ανεξάρτητα από την σύμβαση με τον υπεύθυνο επεξεργασίας

Με αυτόν τον τρόπο ομαλοποιείται η λειτουργία των υπολογιστικών νεφών στις περιπτώσεις όπου ο πελάτης δυσκολεύεται να ελέγξει πλήρως ,τον τρόπο παροχής των τεχνικών μέτρων που λαμβάνει ο πάροχος με σκοπό την διαφύλαξη των προσωπικών δεδομένων . (Μια περίπτωση όπου εμπίπτει σε αυτήν την περίπτωση είναι τα ΜΜΕ )

(ομάδα εργασίας του άρθρου 29,Γνώμη 05/2012 σχετικά με το υπολογιστικό νέφος ]

Στο ίδιο άρθρο του νέου κανονισμού καθιστά υπεύθυνους για την λήψη μέτρων ικανών να επιφέρουν την προστασία των προσωπικών δεδομένων από οποιαδήποτε απειλή που μπορεί να υπάρξει στο διαδίκτυο , τον υπεύθυνο επεξεργασίας αλλά και τον εκτελών την επεξεργασία.

Έτσι παύει να υφίσταται η άνιση μέχρι τώρα θέση που είχαν απέναντι στον νόμο τα πρόσωπα στα οποία αναφέρονται τα δεδομένα , και ο μικρές επιχειρήσεις – χρήστες έναντι των μεγάλων παρόχων υπηρεσιών υπολογιστικού νέφους.

Επιπλέον ο νέος κανονισμός αναγκάζει τις διάφορες οργανώσεις προστασίας των συμφερόντων καταναλωτών και των επιχειρήσεων , να αναλάβουν πιο προορατικό ρόλο στο θέμα της διαπραγμάτευσης και να δημιουργήσουν κατάλληλους όρους στις συναφείς συμβάσεις , όπου να υπάρχουν ισορροπίες μεταξύ των παρόχων υπηρεσιών και των χρηστών .

## 5.2 Κοινοποίηση δεδομένων σε τρίτη χώρα

Μία ακόμα καινοτομία που εισάγει το σχέδιο του νέου Κανονισμού έχει να κάνει με τα ζητήματα λογοδοσίας. Μέχρι σήμερα, σύμφωνα με την Οδηγία 95/46/ΕΚ, αρμόδιο είναι εκείνο το κράτος-μέλος στην επικράτεια του οποίου βρίσκεται ο υπεύθυνος επεξεργασίας. Πλέον με τον νέο κανονισμό θα είναι σε λειτουργία μια ενιαία Αρχή, με ταυτόχρονη ύπαρξη τοπικών γραφείων ελέγχου ανά κράτος-μέλος, όπου θα εφαρμόζονται οι αρχές αυτής αρχής: έτσι, τόσο ο υπεύθυνος επεξεργασίας όσο και ο εκτελών την επεξεργασία είναι υποχρεωμένοι να συμμορφώνονται με την νέα αυτή ενιαία Νομική αρχή .

Ωστόσο δεν αναφέρεται πουθενά στον νέο κανονισμό ότι οι υπεύθυνοι της επεξεργασίας που δραστηριοποιούνται εντός της ΕΕ απαγορεύεται να κοινοποιούν τα δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα βάσει αιτήματος δικαστικής ή διοικητικής αρχής της τρίτης χώρας. Με αυτόν τον τρόπο δημιουργείται ένα μεγάλο κενό στο κατά πόσο είναι ασφαλή τα προσωπικά δεδομένα προσωπικού χαρακτήρα τα οποία αποθηκεύονται σε παρόχους υπολογιστικού νέφους.

Θα πρέπει [Γνώμη05/2012,ομαδα εργασίας του άρθρου 29] να συμπεριληφθεί στον νέο κανονισμό ότι σε περίπτωση επιβολής κοινοποίησης προσωπικών δεδομένων όπου η εφαρμογή της κοινοποίησης δεν είναι σύμφωνη με την νομοθεσία της ΕΕ τότε επιβάλλεται να υπάρξει πριν την κοινοποίηση υποχρέωση αμοιβαίας δικαστικής συνδρομής από ένα δικαστικό φορέα εντός της Ε.Ε.

## 5.3 Τοποθεσία αποθήκευσης των δεδομένων

Ένα ακόμα πολύ σημαντικό θέμα που αφορά το υπολογιστικό νέφος είναι ο τόπος στον οποίο θα βρίσκονται τα δεδομένα, λόγω του ότι θεωρείται αναφαίρετο δικαίωμα του κάθε χρήστη να γνωρίζει το που είναι αποθηκεύονται τα δεδομένα που τον αφορούν.

Πολλοί είναι οι χρήστες που επιθυμούν τα δεδομένα τους να παραμένουν αυστηρά εντός του ευρωπαϊκού χώρου καθώς θεωρούν, και όχι άδικα, ότι σε άλλες χώρες δεν υπάρχει τόσο υψηλό επίπεδο ασφάλειας όσο στην Ευρώπη.

Για να επιλυθεί το παραπάνω πρόβλημα θα πρέπει κατ' αρχάς οι όροι και οι προϋποθέσεις τις σύμβασης μεταξύ πελάτη και παρόχου, να είναι αναλυτικές και κατατοπιστικές. Σημειώνεται ωστόσο ότι πλέον οι περισσότεροι πάροχοι χρησιμοποιούν τυποποιημένες συμβάσεις, οι οποίες πολλές φορές έχουν υποστεί και παρεμβάσεις από τους εκάστοτε αρμόδιους κρατικούς φορείς, με την χρησιμοποίηση των λεγόμενων «γενικών όρων συναλλαγών» (Γ.Ο.Σ) με αποτέλεσμα να μην εξειδικεύουν επαρκώς την σύμβαση. Αυτό όμως παραμένει ένα μείζον θέμα, και για να επιλυθεί θα πρέπει να αλλάξουν οι γενικοί όροι συναλλαγών καθώς και οι προϋποθέσεις της σύναψης των συμβάσεων αυτών έτσι ώστε να μπορέσουν να καλύψουν και τις περιπτώσεις των ζητημάτων που δεν καλύπτονται από το Ευρωπαϊκό δίκαιο, στον τομέα του υπολογιστικού νέφους, συμπεριλαμβανομένου του ζητήματος του τόπου των δεδομένων.

Φυσικά και πάλι θα υπάρχουν έντονες αμφιβολίες, εφόσον ένας πάροχος δραστηριοποιείται και σε χώρες εκτός ευρωπαϊκής ένωσης, περί της αληθινής θέσης των δεδομένων .

## 5.4 Παραβίαση των προσωπικών δεδομένων

Έχουμε ήδη αναφερθεί στη σημαντική καινοτομία που εισάγεται με το νέο κανονισμό σχετικά με τα περιστατικά παραβίασης προσωπικών δεδομένων. Συγκεκριμένα, στο άρθρο 31 του νέου κανονισμού αναφέρεται: «Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας κοινοποιεί στην αρχή ελέγχου την παραβίαση δεδομένων προσωπικού χαρακτήρα αμελλητί και, ει δυνατόν, το αργότερο εντός 24 ωρών από τη στιγμή που την πληροφορείται. Η κοινοποίηση στην αρχή ελέγχου συνοδεύεται από αιτιολογία στις περιπτώσεις στις οποίες δεν πραγματοποιείται εντός 24 ωρών.»

Ως εκ τούτου, στην περίπτωση που ένας πελάτης ενός υπολογιστικού νέφους υποστεί μια παραβίαση στα προσωπικά του δεδομένα, θα πρέπει να γίνει κοινοποίηση της παραβίασης εντός των 24 ωρών.

Εδώ όμως ανακύπτει ένα ζήτημα στην περίπτωση που η επεξεργασία των δεδομένων έχει ανατεθεί σε εξωτερικούς συνεργάτες, οπότε αυτομάτως δυσκολεύεται η έγκαιρη κοινοποίηση για την παραβίαση. Το ζήτημα αυτό επιτείνεται αν αναλογιστεί κανείς την περίπτωση όπου ένας χρήστης έχει αναπτύξει εφαρμογές σε πάροχο υπολογιστικού νέφους, οι οποίες απευθύνονται σε τρίτους. Τότε τον έλεγχο τον εφαρμογών και κατ' επέκταση τον έλεγχο των προσωπικών δεδομένων τον εχει ο χρήστης και καθώς διαφέρει από τον πάροχο υπολογιστικού νέφους υπάρχει έντονα η αμφισβήτηση τι θα γίνει στην περίπτωση της παραβίασης των δεδομένων .

Τελικά, είναι σαφές ότι υπάρχουν δυσκολίες στην πλήρη αφομοίωση των υπηρεσιών υπολογιστικού νέφους εντός της ευρωπαϊκής ένωσης. Ωστόσο, κατ΄αναλογία με το παράδειγμα ότι κανείς πλέον δεν κρατά τα χρήματά του στο σπίτι του αλλά όλοι τα καταθέτουν στην τράπεζα παρόλες τις ενδεχόμενες επιφυλάξεις ή ηθικές αναστολές τους, έτσι το μέλλον τηςυπολογιστικό νέφος ς φαίνεται ότι έχει να δώσει πολλά και όλα εν τέλει θα μπορέσουν να ξεπεραστούν με την βοήθεια της τεχνολογίας.

## 5.5 Δικαίωμα στη λήθη

Επιπλέον ο νεος κανονισμός προωθεί την ελεύθερη και ανοιχτή φύση του διαδικτύου με κύριο στόχο την επίτευξη του δικαιώματος κάθε υποκειμένου, να κρατά στα δικά του χέρια τον πλήρη έλεγχο των προσωπικών του δεδομενων. Για την εφαρμογή αυτών των ρυθμίσεων, επιβάλλεται η δημιουρία ενός νέου βασικού κανόνα, αυτού της δημιουργίας ενός «κουμπιού» διαγραφής ικανού να σβήνει πλήρως και απολύτως ολων αυτών των πληροφοριών που αφορούν ένα «πρόσωπο» και βρίσκονται στο διαδύκτιο. Αυτή είναι η γενική προσέγγιση του δικαιώματος της λήθης.

'Εδω ομως παρουσιάζεται και η πρώτη δυσκολία, ας υποθέσουμε ότι έχουμε μια φωτογραφία στο διαδύκτιο με δύο πρόσωπα επάνω, τον Γιάννη και την Μαρία , και ο Γιάννης ζητήσει την διαγραφή όλων των προσωπικών του δεδομένων, και η Μαρία δεν δεχθεί την διαγραφή της φωτογραφίας , τοτε βρισκόμαστε μπροστά σε μία σύγκρουση των δικαιωμάτων του Γιάννη και της Μαρίας.

Η έννοια του δικαιώματος τη λήθης είναι μεν πολύ εύλογη και εύστοχη ως προς την θεωρία . Η εφαρμογή του όμως με τα δεδομένα τεχνικά μέσα και η νομική κατοχύρωση εφαρμογή του, χρήζει άμεσα από κάποιες διευκρινίσεις :

- Ποιος έχει το δικαίωμα να ζητήσει την διαγραφή των προσωπικών του δεδομένων
- Ποιες είναι η συνθήκες κάτω από τις οποίες μπορεί κάποιος να ζητήσει την διαγραφή των δεδομένων του
- Ποιοι είναι οι αποδεκτοί τρόποι όπου μπορεί κανείς να διαγράψει τα δεδομένα του χωρίς να επηρεάσει το υπόλοιπο διαδικτυακό χώρο

Οποιαδήποτε νομικό ορισμό και εάν δώσουμε στο δικαίωμα της λήθης , καταλαβαίνουμε ότι η εφαρμογή του σε ένα ανοιχτό διεθνές Διαδίκτυο είναι τουλάχιστον δυσχερής έως αδύνατη.

Μερικές πιθανές προσεγγίσεις για την εφαρμογή της υλοποίησης του δικαιώματος της λήθης είναι :

- Ένα μεγάλο ρόλο κατά την εφαρμογή του δικαιώματος της λήθης παίζουν οι πάροχοι των μηχανών αναζήτησης του διαδικτύου , [Η ομάδα εργασίας του άρθρου 29 τους , Γνώμη 1/2008 ] τονίζει την μέγιστη σημασία των παρόχων των μηχανών αναζήτησης καθώς διαδραματίζουν βασικό ρόλο στην κοινωνία της πληροφορίας ως μεσολαβητές. Η χρησιμότητα των μηχανών αναζήτησης είναι η μέγιστη και συμβάλλουν στην ανάπτυξη της κοινωνίας της πληροφορίας και κατ' επέκταση στο ίδιο το διαδίκτυο.
- Ο χάρτης των θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, στο άρθρο 11 προβλέπει ότι η πρόσβαση στις πληροφορίες πρέπει να είναι ελεύθερη και να μην παρακολουθείται από τις δημόσιες αρχές ,καθώς αποτελεί μέρος της ελευθερίας της έκφρασης και της πληροφόρησης.[ Ευρωπαϊκό Κοινοβούλιο , Χάρτης των Θεμελιωδών Δικαιωμάτων της ΕΕ]. Έτσι εδώ παρατηρούμε ότι απαιτείται ο πλήρης ορισμός της επιτρεπτής επεξεργασίας των προσωπικών δεδομένων, γιατί σε αντίθετη περίπτωση ενδεχομένως να υπάρχει σύγκρουση με το επίσης Ευρωπαϊκά κατοχυρωμένο δικαίωμα στην πληροφορία.

- Έχοντας σαν γνώμονα τους δύο ορισμούς η προσπάθεια της εφαρμογής του δικαιώματος της λήθης, θα επικεντρωθεί σε τεχνικά εργαλεία τα οποία είναι ήδη διαθέσιμα και μπορούν να εφαρμοστούν στις μηχανές αναζήτησης , έτσι ώστε να μπορέσει να ενισχυθεί η αναλυτικότητα και η αποτελεσματικότητα της αναζήτησης του χρήστη.

### 5.5.1 Τεχνικά ζητήματα στην εφαρμογή της λήθης

Μερικά ακόμα τεχνικά ζητήματα που θα πρέπει να εξεταστούν για την εφαρμογή του δικαιώματος της λήθης είναι :

1) Να μπορέσει ο χρήστης να αναγνωριστεί και να προσδιοριστεί όταν απαιτείται, δηλαδή επαρκή ταυτοποίηση του χρήστη
2) Να εντοπιστούν πλήρως όλα τα προσωπικά δεδομένα του υποκειμένου που ζητήθηκε, οπουδήποτε στο διαδίκτυο και εάν βρίσκονται αυτά
3) Επιπλέον να γίνει ο πλήρης εντοπισμός και όλων των αντιγράφων ασφαλείας των προσωπικών δεδομένων του υποκειμένου στο διαδίκτυο
4) Να καθοριστεί ο τρόπος με τον οποίο θα ζητά ένα πρόσωπο την διαγραφή των προσωπικών του δεδομένων.
5) Να καθοριστεί η εξακρίβωση του χρήστη, και εάν έχει ο συγκεκριμένος χρήστης το δικαίωμα να πραγματοποιήσει την διαγραφή των δεδομένων που ζητά .

### 5.5.2 Πρωτόκολλο αποκλεισμού ΡΟΜΠΟΤ

Μια πιθανή λύση για την επίτευξη του δικαιώματος της λήθης είναι με την βοήθεια του πρωτόκολλου αποκλεισμού Ρομπότ ( robots.txt.), το οποίο είναι ένα διαδικτυακό ρομπότ που ήδη χρησιμοποιείται ευρέως από τους διαχειριστές των ιστοσελίδων το οποίο που εκτελεί αυτοματοποιημένες εργασίες μέσα στο διαδίκτυο.

Οι διάφοροι web servers δημιουργούν ένα απλό αρχείο κειμένου με το όνομα "robots.txt", το οποίο περιέχει κανόνες που θα πρέπει να τηρήσουν τα διάφορα bots (αυτοματοποιημένα εργαλεία bots) που επισκέπτονται την σελίδα .

Έπειτα το αρχείο robot κάνει επίσκεψη στη διεύθυνση URL της τοποθεσίας της ιστοσελίδας σας, ας πούμε ότι αυτή είναι η:

http://www.example.com/welcome.html.

Πριν λοιπόν διαβάσει την διεύθυνσή σας το robot διαβάζει πρώτα τον εαυτό του που είναι το:

http://www.example.com/robots.txt και διαπιστώνει τα εξής:

| |
|---|
| User-agent: * |
| Disallow: / |
| The "User-agent: *" means this section applies to all robots. The "Disallow: /" tells the robot that it should not visit any pages on the site. |
| (Στον "User-agent: *" σημαίνει ότι αυτή η ενότητα ισχύει για όλα τα ρομπότ. Το "Disallow: /" λέει στο ρομπότ ότι δεν θα πρέπει να επισκεφθεί σελίδες του δικτυακού τόπου.) |

Θα πρέπει να δοθεί ιδιαίτερη προσοχή στον τρόπο που θα γραφεί το αρχείο του robots.txt , ιδίως όσον αφορά την λεξιλογική και σημασιολογική ορθότητα των οδηγιών του, προς αποφυγή αντικρουόμενων ή τυχόν επικαλυπτόμενων οδηγιών. Καθώς με την χρήση του πρωτοκόλλου robots .txt, ένα ρομποτικό πρόγραμμα αναλαμβάνει να αποφασίσει εάν θα εμφανιστούν τα περιεχόμενα των διαφόρων ιστοσελίδων στις μηχανές αναζήτησης ή θα εμφανιστούν μόνο στην οθόνη του χρήστη.

Ένα ακόμα αξιοσημείωτο θέμα που αφορά το πρωτόκολλο robots.txt είναι ότι η χρήση του γίνεται σε περιορισμένα θέματα και δεν προσφέρεται για πρόσβαση σε περιεχόμενα όπως τα δεδομένα της κινητής τηλεφωνίας ,όπως τα sms ή τα αποθηκευμένα e-mail ή τα δεδομένα ανίχνευσης τοποθεσίας.

Και επιπλέον δεν μπορεί να έχει πλήρη πρόσβαση στις ρυθμίσεις των διαφόρων ιστοσελίδων, αλλά είναι στην ευχέρεια του κάθε διαχειριστή των ιστοσελίδων να αποφασίζει μέχρι ποιον βαθμό θα επιτραπεί η χρήση του πρωτοκόλλου robox.txt. στην ιστοσελίδα του, και μέχρι ποιες πληροφορίες θα διαβάσει το robox.txt.

Μέχρι σήμερα η επικρατέστερη πιθανή εκδοχή εφαρμογής το δικαιώματος της λήθης είναι με την εφαρμογή προγράμματος robots, με σκοπό να αποκρύπτονται οι

πληροφορίες οι οποίες θα βρίσκονται σε λήθη. Έτσι με την χρήση του θα επιτραπεί στους χρήστες του διαδικτύου να ασκούν το δικαίωμα τους να ξεχαστούν .

Όμως η αυθαίρετη αφαίρεση ιστοσελίδων από το διαδίκτυο, ή η απόκρυψη διαφόρων πληροφοριών από τους χρήστες αυτομάτως παρεμποδίζει την ελευθερία της πληροφορίας, και είναι βέβαιο ότι θα έχει αντίκτυπο στο γενικότερο δυναμικό του ιντερνέτ και σαφώς θα κλονιστεί η οικονομία των διάφορων επιχειρησιακών μοντέλων που στηρίζονται στην πληροφόρηση.

Η αρχική ιδέα του δικαιώματος της λήθης όριζε ένα κουμπί διαγραφής ικανό να διαγράφει όλες τις πληροφορίες από οποιοδήποτε μέρος του διαδικτύου σχετικά με κάποιον, με την εφαρμογή του πρωτοκόλλου ρομπότ, οι πληροφορίες αυτές, αποκρύπτονται μεν , αλλά δεν διαγράφονται και έτσι υπάρχουν έντονες αμφιβολίες, κατά πόσο υλοποιήσιμη είναι τελικά η ιδέα του ορισμού της λήθης, ή έστω και κατά πόσο είναι πρακτικά εφαρμόσιμη σε ένα ανοιχτό διαδίκτυο. Τέλος τα περιεχόμενα του αρχείου robots.txt είναι πολύ πολύτιμα στους διάφορους χάκερ του διαδικτύου καθώς και σε οποιαδήποτε οντότητα που επιδιώκει να διαδώσει / αποσπάσουν προσωπικά δεδομένα.

## 5.6 Μηχανές αναζήτησης και επεξεργασίας δεδομένων

Οι μηχανές αναζήτησης επεξεργάζονται τις γενικές πληροφορίες αλλά και μεταξύ των άλλων και τις προσωπικές πληροφορίες , διερευνώντας , αναλύοντας , και ευρετηριάζοντας τον παγκόσμιο ιστό και άλλες πηγές τις οποίες καθιστούν εύχρηστες, και επομένως ευπρόσιτες μέσω αυτών των υπηρεσιών. Ορισμένες υπηρεσίες μηχανής αναζήτησης αναδημοσιεύουν επίσης τα δεδομένα στην καλούμενη «κρυφή μνήμη» [ομάδα εργασίας άρθρου 29,] Επιπλέον η ομάδα εργασίας του άρθρου 29 τονίζει ότι οι μηχανές αναζήτησης δεν εμπίπτουν στο πεδίο εφαρμογής του ορισμού των υπηρεσιών ηλεκτρονικών επικοινωνιών. Κάτι το οποίο ενστερνίζεται και ο γενικός εισαγγελέας του Δικαστηρίου της Ευρωπαϊκής Ένωσης που θεωρεί ότι βάσει της οδηγίας 95/46 οι πάροχοι υπηρεσίας μηχανής αναζήτησης στο Διαδίκτυο δεν φέρουν ευθύνη για την προστασία δεδομένων προσωπικού χαρακτήρα που εμφανίζονται σε ιστοσελίδες τις οποίες επεξεργάζονται.

Η εθνική νομοθεσία για την προστασία δεδομένων έχει εφαρμογή επί των εν λόγω παρόχων όταν ιδρύουν σε ένα κράτος μέλος γραφείο το οποίο κατευθύνει τη δραστηριότητά του στον πληθυσμό του οικείου κράτους, με σκοπό την προώθηση και την πώληση διαφημιστικού χώρου, ακόμη και αν από τεχνική άποψη η επεξεργασία των δεδομένων εκτελείται σε άλλο τόπο.[ Ασφάλεια στο διαδίκτυο, Κυριακή, 30 Ιουνίου 2013 ]

Ωστόσο , υπάρχουν ορισμένα είδη επεξεργασίας, την οποία εκτελούν ξεχωριστά ως ελεγκτές δεδομένων και έτσι μπορεί ένας πάροχος υπηρεσίας μηχανής αναζήτησης να αποσύρει πληροφορίες από το ευρετήριο του , σε περιπτώσεις όπου έχει δεχτεί αίτημα αποκλεισμού από κάποιον ιστότοπο.

Έτσι θα πρέπει να δοθεί ιδιαίτερη σημασία στην λειτουργία αποθήκευσης σε κρυφή μνήμη καθώς αποτελεί άλλον έναν τρόπο με τον οποίο ένας πάροχος μηχανής αναζήτησης μπορεί να υπερβεί τον ρόλο του ως αποκλειστικά μεσολαβητή. Η περίοδος διατήρησης του περιεχομένου σε κρυφή μνήμη θα πρέπει να περιορίζεται στο χρονικό διάστημα που είναι απαραίτητο για να αντιμετωπισθεί το πρόβλημα προσωρινής αδυναμίας πρόσβασης στον δικτυακό τόπο. [ομάδα εργασίας άρθρου 29]

Ο πιο πιθανός τρόπος που θα μπορέσει να μας οδηγήσει στην επίτευξη του δικαιώματος της λήθης είναι αρχικά η χρήση τεχνολογιών όπου θα υποστηρίζουν την αρχή της ελάχιστης γνωστοποίησης προκειμένου να ελαχιστοποιηθεί ο όγκος των προσωπικών δεδομένων προσωπικού χαρακτήρα τα οποία συλλέγονται και αποθηκεύονται ηλεκτρονικά, και έπειτα η αναπροσαρμογή των μηχανών αναζήτησης ως ελεγκτών δεδομένων :

- Οι μηχανές αναζήτησης θα πρέπει να εφαρμόσουν ειδικά προγράμματα ανίχνευσης. Για να μπορούν να ομαδοποιούν δεδομένα βάσει των διαφόρων κατηγοριών και για διαφορετικούς σκοπούς ( γενικά ευρετηρίασης , ειδήσεις , εικόνες , κλπ. ) , ώστε να επιτρέπουν στους διαχειριστές των ιστοσελίδων να ελέγχουν καλύτερα τις πληροφορίες που θέλουν να δημοσιεύονται.

- Επιπλέον κατά την φάση της ευρετηρίασης των ιστοσελίδων , οι μηχανές αναζήτησης θα πρέπει να μπορούν να δέχονται πιο περίπλοκες και πιο αναλυτικές οδηγίες στα λογισμικά ανίχνευσής τους στο διαδίκτυο.

- Όταν ένα πρόγραμμα ανίχνευσης στο διαδίκτυο (crawling) ακολουθείται από την προσωρινή αποθήκευση της ιστοσελίδας για διαφορετικούς σκοπούς από τους σκοπούς που έχουν αποδεχθεί οι χρήστες , οι μηχανές αναζήτησης θα πρέπει να παρέχουν στους διαχειριστές της συγκεκριμένης ιστοσελίδας σαφείς πληροφορίες σχετικά με το χρονοδιάγραμμα και τους τεχνικούς μηχανισμούς που ισχύουν στην κρυφή μνήμη για τα δεδομένα που αποθηκεύτηκαν.

- Τελευταίο αλλά πολύ σημαντικό είναι ότι οι μηχανές αναζήτησης θα πρέπει να μπορούν να διαγράφουν αμέσως, οποιοδήποτε αποθηκευμένο αντίγραφο των δεδομένων τους όταν υπάρξει ένα αίτημα διαγραφής από έναν υπεύθυνο επεξεργασίας ενός διαδικτυακού τόπου. Μειώνοντας έτσι το ρίσκο της διάδοσης των δεδομένων χωρίς έγκριση .

# Κεφάλαιο 6
# Σύνοψη -Συμπεράσματα

Ο νέος κανονισμός που προτείνεται από την Ευρωπαϊκή Επιτροπή, συμβάλει ακόμα περισσότερο στην πληρέστερη κατοχύρωση των δικαιωμάτων των πολιτών της Ευρωπαικής Ένωσης, κατοχυρώνοντας την πληρέστερη προστασία προσωπικών δεδομένων που έχει ψηφιστεί εως σήμερα. Είναι ένα βήμα προς την σωστή κατεύθυνση, με στόχο να επιτευχθεί τελικά ένας χώρος ελευθερίας ασφάλειας και δικαιοσύνης ένας στόχος που ορίζεται στο άρθρο 2 της **Συνθήκης της Λισαββώνας.**[17]

Έτσι η ενοποίηση της νομοθεσίας με την εφαρμογή ενός και μόνο κανονισμού σε όλη την Ευρωπαϊκή Ένωση αντίθετα με τις ισχύουσες σήμερα εκάστοτε διαφορετικές εθνικές νομοθεσίες των κρατών, θα δώσει μεγαλύτερη ασφάλεια δικαίου, μέσα από την ενοποίηση της νομολογίας κάτι το οποίο θα δώσει ώθηση και στην ενιαία αγορά, αφού θα είναι ευκολότερο για μια εταιρία να έχει πρόσβαση σε νέες αγορές. Ενώ και η δημιουργία μιας μόνο υπεύθυνης αρχής σε κάθε κράτος θα βοηθήσει προς αυτή την κατεύθυνση.

Καθώς και οι νέες πληρέστερες ρυθμίσεις οι οποίες ορίζουν αυστηρότερες προϋποθέσεις ευθύνης και λογοδοσίας για τους υπεύθυνους επεξεργασίας και τους παρέχων την επεξεργασία,

Όμως, παρά τις αρκετά ικανοποιητικές και εύστοχες ρυθμίσεις του Ευρωπαίου Νομοθέτη σε πολλά σημεία, βλέπουμε ότι τελικά το νομικό σύστημα σαν τέτοιο, δηλαδή σαν νομικοί κανόνες προστασίας των πολιτών, έχει φτάσει στα όρια του. Με την έννοια ότι δεν υπάρχουν μέχρι σήμερα οι τεχνολογικές λύσεις για να εφαρμόστουν πλήρως αυτές οι νομοθετικές ρυθμίσεις, και έτσι να κατοχυρώθούν πλήρως τα δικαιώματα που προσπαθεί να προστατέψει η Ευρωπαϊκή Ένωση. Για παράδειγμα η προσπάθεια της εφαρμογής του δικαίωματος στην λήθη, με την χρήση του πρωτοκόλου ρομπότ, έχει φτάσει στα όρια του δεδομένο ότι αυτό το πρωτόκολο έχει σχεδιαστεί πριν από σχεδόν 15 χρόνια και υποστηρίζει μόνο απλές εντολές και επιλογές.
Αντίθετα η χρήση αλγορίθμων ενσωματωμένων σε κάθε πληροφορία την οποία αναρτούμε στο διαδίκτυο τα οποία θα επιτρέπουν τον έλεγχο στην πρόσβαση σε αυτές τις πληροφορίες και η χρήση πιο προηγμένεων αλγόριθμων και λογισμικών στης μηχανές αναζήτησης με σκοπό να φιλτράρουν ακόμα πιο πολύ τις πληροφορίες και να δίνουν περισσότερες επιλογές εμφάνισης τους ή όχι αλλά και την εξακρίβωση εάν κάποιος είναι ο κάτοχος μιας πληροφορίας και κατ' επέκταση έχει το δικαίωμα να την αφαιρέσει ή όχι, η ακόμα και αν ισχεί ακόμη, φαίνεται πιο λειτουργικός τρόπος ωστόσω απαιτείται η περαιτέρω ανάπτυξη τέτοιων λογισμικών τα οποία όμως βρίσκοντα ακόμα σε αρχικό στάδιο.
Δηλαδή καταλήγουμε σε αυτό το οποίο έχει δηλώσει ό πρόεδρος της ENISA ότι τελικά το δικαίωμα στην λήθη είναι πρακτικά αδύνατο να υλοποιηθεί με τα σημερινά τεχνικά μέσα.

Κατ'επέκταση κατανοούμε ότι το δικαίωμα στην λήθη είναι αδύνατο στο ανοικτό, παγκόσμιο σύστημα που υφίσταται σήμερα, και ηικανότητα να υλοποιηθεί το «δικαίωμα να λησμονηθούν» εξαρτάται σε μεγάλο βαθμό από τις τεχνικές δυνατότητες του βασικού συστήματος πληροφοριών, και τις δομές δεδομένων του δικτύου

Αυτό συμβαίνει διότι ο παγκόσμιος ιστός είναι ένα ανοιχτό σύστημα οπου ο καθένας μπορεί να αντιγράφει στοιχεία από δημόσια δεδομένα , και να τα αποθηκεύει σε αυθαίρετες τοποθεσίες του ιστού. Επιπλέον σε αυτό το σύστημα είναι πολύ δύσκολο

να καθοριστεί αν ένα πρόσωπο έχει το δικαίωμα να ζητήσει την αφαίρεση ενός συγκεκριμένου στοιχείου δεδομένων, ενώ επίσης είναι δυσχερές να πουμε ότι κάθε μεμονωμένο πρόσωπο ή οντότητα έχει την εξουσία ή τη δικαιοδοσία να πραγματοποιήσει την διαγραφή όλων των αντιγράφων.

# Βιβλιογραφία


[01] EU Data Protection Directive 95/46/EC (Official Journal of the European Communities of 23 November 1995.

[02] Proposal for a Regulation of the European Parliament on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM 2012/0011)

[03] Αρχή προστασίας προσωπικών δεδομένων , [http://www.dpa.gr]

[04] Article 29 Data Protection Working Party, "Opinion 05/2012 on cloud computing"

[05] Article 29 Data Protection Working Party, "Opinion 04/2012 on cookie consent exemption"

[06] Article 29 Data Protection Working Party, "Opinion 02/2012 on facial recognition in online and mobile services"

[07] Article 29 Data Protection Working Party, "Opinion 05/2009 on online social networking"

[08] Enisa , European Network and Information Security Agency ,The right to be forgotten – between expectations and practice.

[09] Γνωμοδότηση 01/2012 σχετικά με τις προτάσεις μεταρρύθμισης της προστασίας των δεδομένων"

[10] European Commission, How will the EU's data protection reform make international cooperation easier (Πώς η μεταρρύθμιση του καθεστώτος προστασίας δεδομένων της ΕΕ θα απλοποιήσει τους υφιστάμενους κανόνες; )

[11] Ευρωπαϊκή επιτροπή, "Γιατί είναι αναγκαία η μεταρρύθμιση του καθεστώτος προστασίας δεδομένων της ΕΕ;"

[12] Ευρωπαϊκή επιτροπή, “Με ποιο τρόπο η μεταρρύθμιση του καθεστώτος προστασίας δεδομένων ενισχύει τα δικαιώματα των πολιτών;”

[13] Ευρωπαϊκή επιτροπή, " Πώς η μεταρρύθμιση του καθεστώτος προστασίας δεδομένων της ΕΕ θα απλοποιήσει τους υφιστάμενους κανόνες;”

[14] Ευρωπαϊκή επιτροπή, " Πώς επωφελούνται οι ευρωπαϊκές επιχειρήσεις από την μεταρρύθμιση του καθεστώτος προστασίας δεδομένων της ΕΕ”

[15] «Εισαγωγή στο Ευρωπαϊκό Δίκαιο» *Δονάτος Παπαγιάννης, Δεύτερη έκδοση, Εκδόσεις Αντ. Ν .Σάκκουλα 1999, ISBN: 960-15-0133-9*

[16] «Συνταγματικό Δίκαιο – Ατομικά Δικαιώματα» *Π. Δ. Δαγτόγλου, Δεύτερη έκδοση, Εκδόσεις Αντ. Ν .Σάκκουλα 2005, ISBN: 960-15-1371-X*

[17] Η Συνθήκη της Λισαβόνας, 13-12-2007 [http://bookshop.europa.eu/is-bin/INTERSHOP.enfinity/WFS/EU-Bookshop-Site/el_GR/-/EUR/ViewPublication-Start?PublicationKey=FXAC07306]

[18] INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS “Draft Working Paper and Recommendations on Website Contents Indexing and Protection of the “Right to Be Forgotten” 52st Meeting – Berlin, 10-11 September 2012

[19] Ευρωπαϊκό κοινοβούλιο, Προσωπικά δικαιώματα πόσο προσωπικά είναι ; [http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//TEXT+IMPRESS+20130521FCS08720+0+DOC+XML+V0//EL]

[20] Ευρωπαϊκό Κοινοβούλιο , Χάρτης των Θεμελιωδών Δικαιωμάτων της ΕΕ.

[21] Ομάδα εργασίας του άρθρου 29, «Γνώμη 1/2008 σχετικά με τα θέματα προστασίας δεδομένων σε σχέση με τις μηχανές αναζήτησης»

[22] Wikipedia, Διαδικτυακό Ρομπότ.

[23] CnC Tech block , Pavlos Chatzipapas ,Οκτώβριος 16 ,
[http://cnctech.gr/blog/sxetika-me-ta-robots-txt]

[24] Ιωάννη Δ. Ιγγλεζάκη Δικηγόρου – Καθηγητή ΑΠΘ , Το δικαίωμα στην ψηφιακή λήθη.
[http://informaticslaw.blogspot.gr/2012/11/to.html]

[25] Ομάδα εργασίας του άρθρου 29 «Γνώμη 8/2010 για το εφαρμοστέο δίκαιο»
[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_el.pdf]

[26] Ασφάλεια στο διαδίκτυο, Κυριακή, 30 Ιουνίου 2013
[http://internet-safety.sch.gr/index.php/articles/parents/item/238-srcheng]

[27] Σύνταγμα της Ελλάδας, ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ

[28] Ευρωπαϊκή σύμβαση για τα δικαιώματα του ανθρώπου, [http://el.wikipedia.org]

[29] ΓΡΑΦΕΙΟ ΕΠΙΤΡΟΠΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ
[http://www.dataprotection.gov.cy]

[30] E-Lawyer, [ένα νομικό ιστολόγιο για τα ανθρώπινα δικαιώματα στην ψηφιακή εποχή]
[http://elawyer.blogspot.gr/]

[31] Warren & Brandeis, The Right of Privacy, 4 Harv. L. Rev. 193 (1890)
[http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm]

[32] California Law Review August 1960 Vol48, no3, Privacy, William L. Prosser
[http://www.californialawreview.org/assets/pdfs/misc/prosser_privacy.pdf]

[33] Privacy as an aspect of human dignity: an answer to dean Prosser Edward J. Bloustein
[http://courses.ischool.berkeley.edu/i205/s10/readings/week11/bloustein-privacy.pdf]

[34] Ασφάλεια δεδομένων στην κοινωνία της πληροφορίας, Καλλονιάτης Χρήστος,
Λέκτορας Τμήμα Πολιτισμικής Τεχνολογίας και Επικοινωνίας, Πανεπιστήμιο Αιγαίου
[http://www.ct.aegean.gr/people/kalloniatis]

[35] http://el.wikipedia.org/wiki/Απειλές και μηχανισμοί προστασίας της ιδιωτικότητας σ τα ασύρματα και κινητά δίκτυα

[36] Βενιαμίν Φραγκλίνος http://en.wikiquote.org/wiki/Benjamin_Franklin

[37] Ευρωπαϊκό Κοινοβούλιο, Προσωπικά δεδομένα: πόσο προσωπικά είναι; [http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20130521FCS08720+0+DOC+XML+V0//EL]